CISA | CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY

SOLUTIONS FOR THE TARGETED VIOLENCE THREAT

PROACTIVE PREPARATION
TO MANAGE THE UNTHINKABLE

CYBERSECURITY &
INFRASTRUCTURE
SECURITY AGENCY

Cybersecurity and Infrastructure Security Agency (CISA)

VISION

Secure and resilient infrastructure for the American people.

MISSION

CISA partners with industry and government to understand and manage risk to our Nation's critical infrastructure.

OVERALL GOALS

GOAL 1

DEFEND TODAY

Defend against urgent threats and hazards

seconds | days | weeks

GOAL 2

SECURE TOMORROW

Strengthen critical infrastructure and address long-term risks

months | years | decades

CISA Operational Priorities

CYBER SUPPLY CHAIN AND 5G

CISA is focused on supply chain risk management in the context of national security. CISA is looking to reduce the risks of foreign adversary supply chain compromise in 5G and other technologies.

ELECTION SECURITY

CISA assists state and local governments and the private sector organizations that support them with efforts to enhance the security and resilience of election infrastructure. CISA's objective is to reduce the likelihood of compromises to election infrastructure confidentiality, integrity, and availability, essential to the conduct of free and fair democratic elections.

SOFT TARGET SECURITY

As the DHS lead for the soft targets and crowded places security effort, CISA supports partners as they identify, develop, and implement innovative and scalable measures to mitigate risks to these venues; many of which serve an integral role in the country's economy.

FEDERAL CYBERSECURITY

CISA provides technology capabilities, services, and information necessary for agencies across the Federal civilian executive branch to manage sophisticated cybersecurity risks. CISA's authorities enable deployment of robust capabilities to protect Federal civilian unclassified systems, recognizing that continuous improvement is required to combat evolving threats. CISA also works to help State, Local, Tribal and Territorial governments improve cybersecurity and defend against cybersecurity risks.

INDUSTRIAL CONTROL SYSTEMS

CISA leads the Federal Government's unified effort to work with the Industrial Control Systems (ICS) community to reduce risk to our critical infrastructure by strengthening control systems' security and resilience.

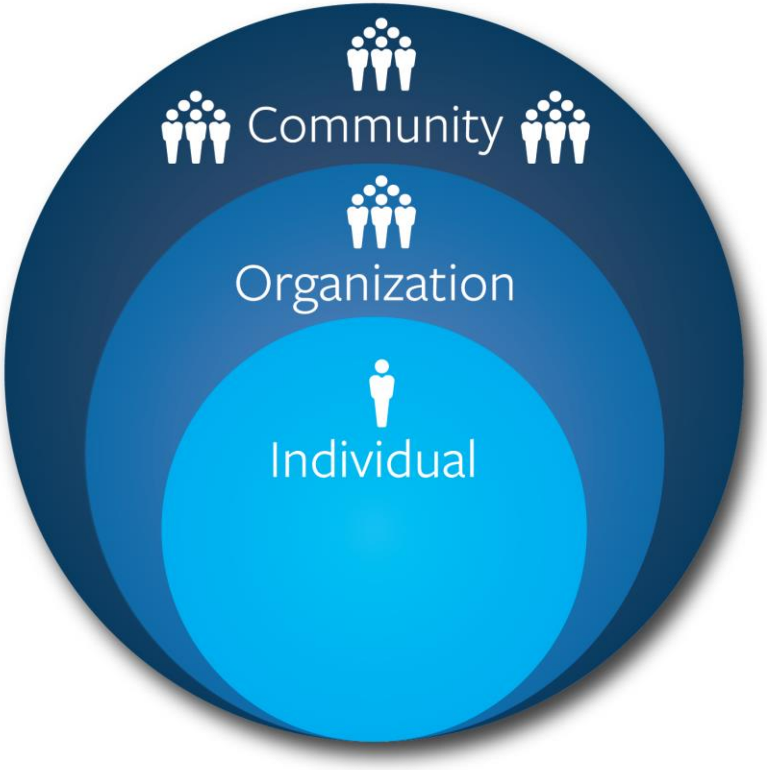
Takeaways Today

Recognition
understand the Targeted Violence threat

Prevention
recognize, report, intervene, mitigate

Preparedness
Build and implement TWO plans

1. Security Plan
2. Emergency Response Plan



Make Two Plans

Security Plans:

- Identify threats and vulnerabilities
- Assess Risk
- Outline a strategy for using layers of security
- Exercise the Plan

Emergency Plans:

- Receive alerts and warnings
  - Find Shelter
  - Carry Out Evacuation
- Communicate with Staff
- Have First Aid
- Assign Courses of Action
- Exercise the Plan

Preparedness Planning

Shootings seem unpredictable, but prevention does not require prediction.

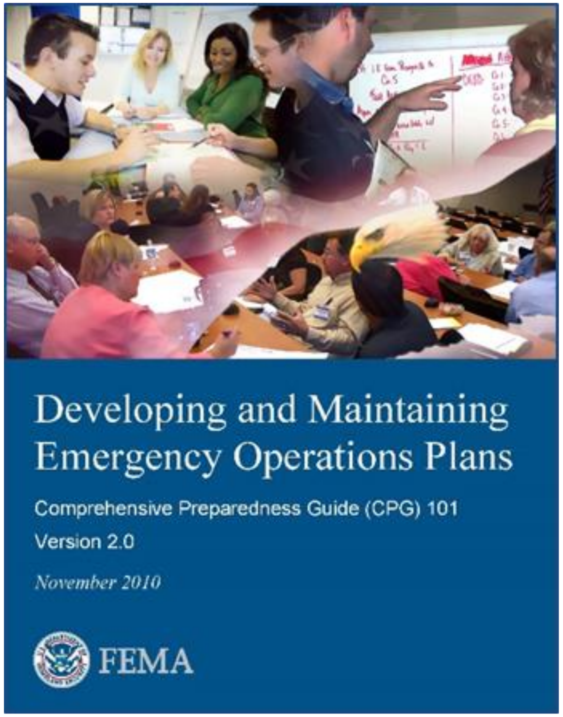
- Dr. Dewey Cornell

Comprehensive School Threat Assessment Guidelines (CSTAG)

Active Shooter Preparedness Plan

A plan will typically address five areas:

- **Prevention**
- **Protection**
- **Mitigation**
- **Response**
- **Recovery**



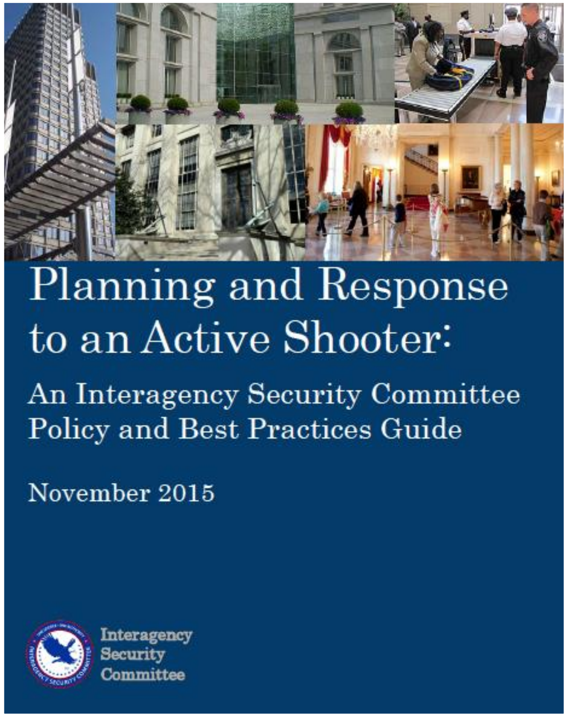
Developing and Maintaining Emergency Operations Plans

Comprehensive Preparedness Guide (CPG) 101

Version 2.0

November 2010

FEMA



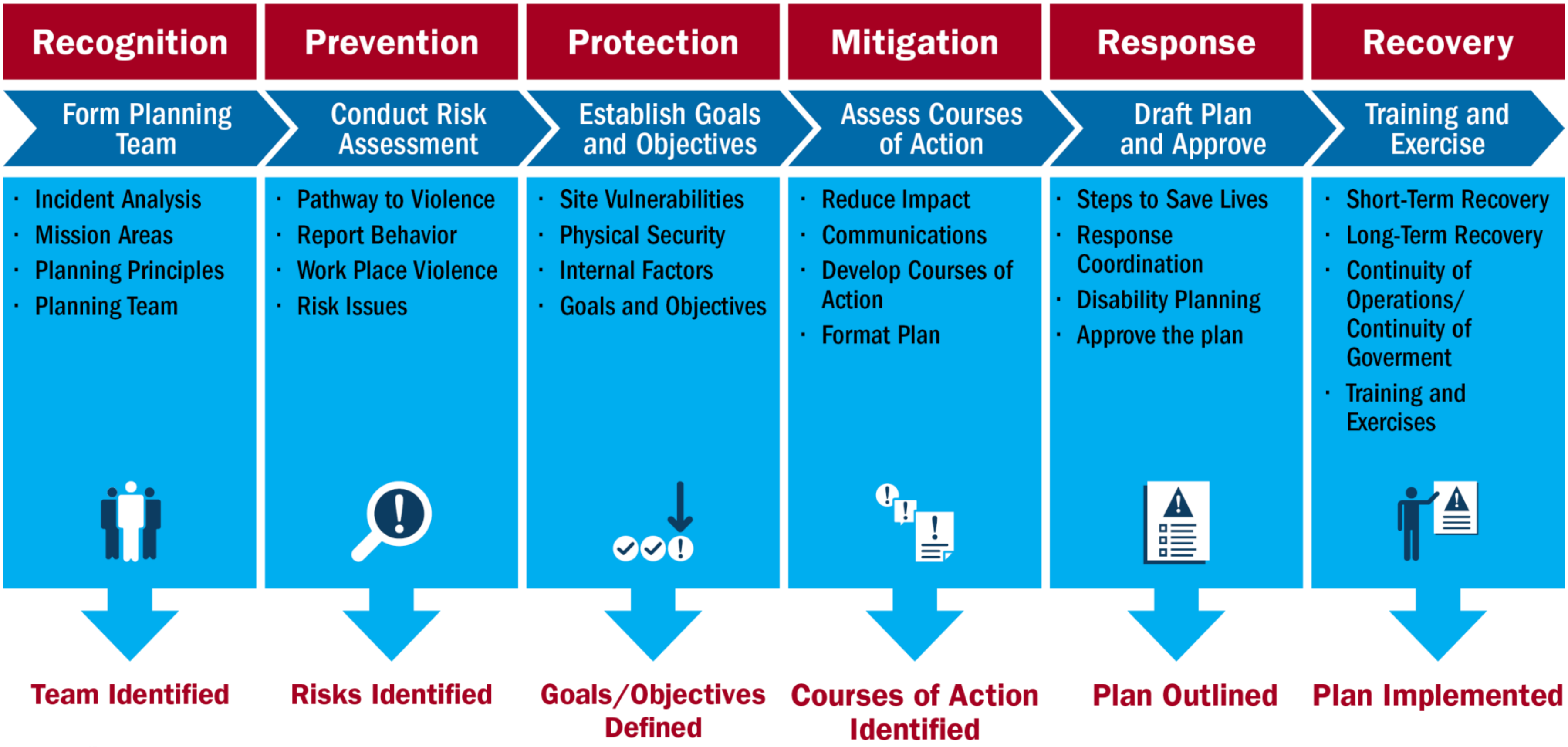
Planning and Response to an Active Shooter:

An Interagency Security Committee Policy and Best Practices Guide

November 2015

Interagency
Security
Committee

Presentation Overview



Recognition

Form Planning Team

- Incident Analysis
- Mission Areas
- Planning Principles
- Planning Team

Team Identified

Prevention

Conduct Risk Assessment

- Pathway to Violence
- Report Behavior
- Work Place Violence
- Risk Issues

Risks Identified

Protection

Establish Goals and Objectives

- Site Vulnerabilities
- Physical Security
- Internal Factors
- Goals and Objectives

Goals/Objectives Defined

Mitigation

Assess Courses of Action

- Reduce Impact
- Communications
- Develop Courses of Action
- Format Plan

Courses of Action Identified

Response

Draft Plan and Approve

- Steps to Save Lives
- Response Coordination
- Disability Planning
- Approve the plan

Plan Outlined

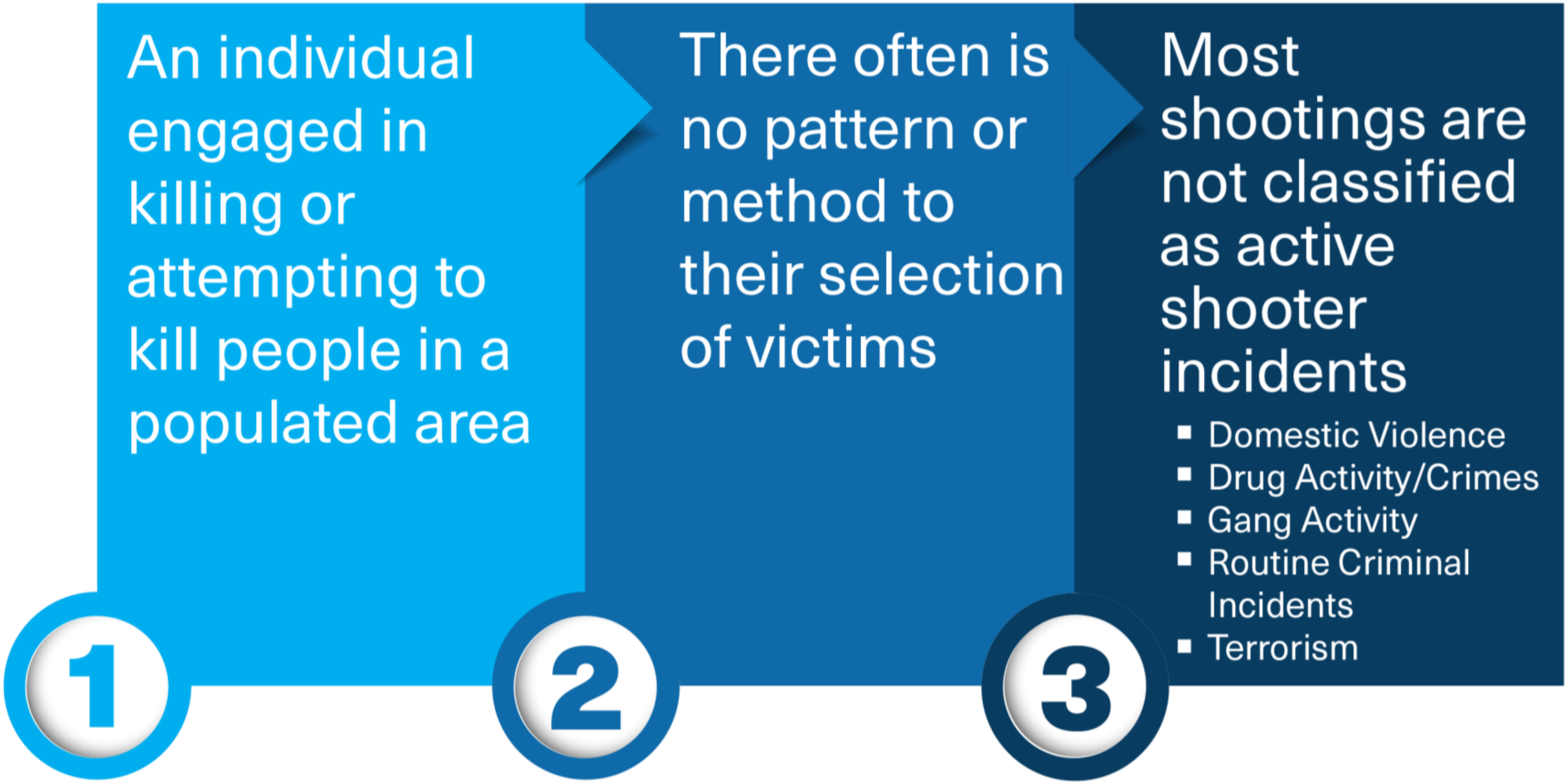
Recovery

Training and Exercise

- Short-Term Recovery
- Long-Term Recovery
- Continuity of Operations/ Continuity of Goverment
- Training and Exercises

Plan Implemented

Active Shooter



1. An individual engaged in killing or attempting to kill people in a populated area

2. There often is no pattern or method to their selection of victims

3. Most shootings are not classified as active shooter incidents
   - Domestic Violence
   - Drug Activity/Crimes
   - Gang Activity
   - Routine Criminal Incidents
   - Terrorism

Active Shooter Timeline

1966 Texas Tower (Austin, TX)

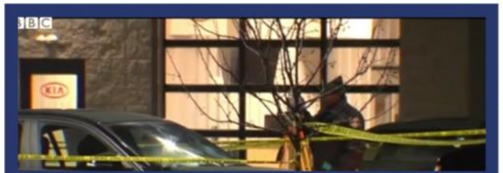
1984 San Ysidro (San Diego, CA)

1999 Columbine H.S. (Littleton, CO)

2007 Virginia Tech (Blacksburg, VA)

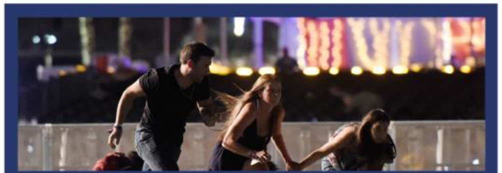
2012 Aurora Theater (Aurora, CO)

2013 Navy Yard (Washington, DC)



2016 Kalamazoo (Kalamazoo, MI)

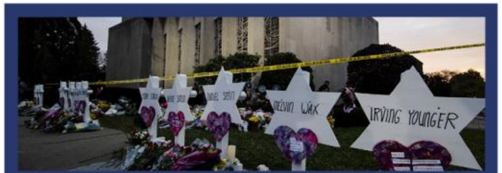
2017 Pulse Nightclub (Orlando, FL)



2017 Harvest Festival (Las Vegas, NV)

2018 Stoneman Douglas HS (Parkland, FL)

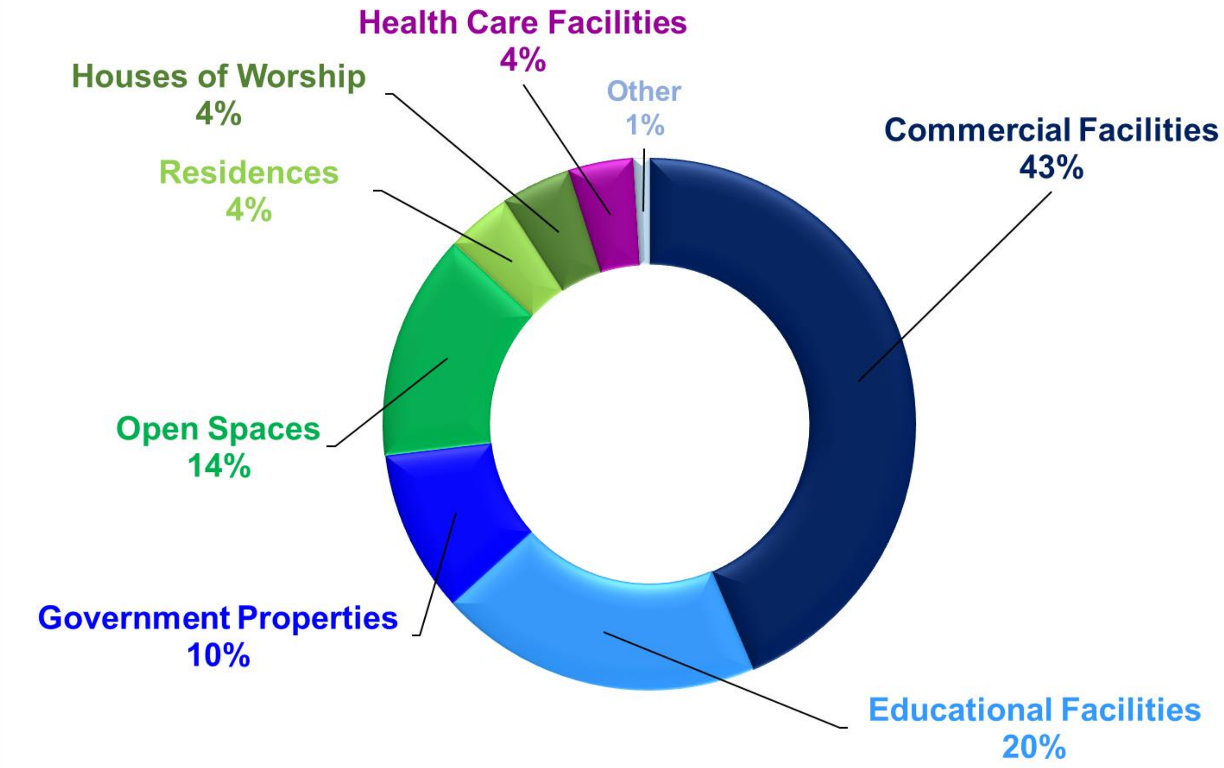
2018 Capital Gazette (Annapolis, MD)



2018 Tree of Life Synagogue (Pittsburgh, PA)

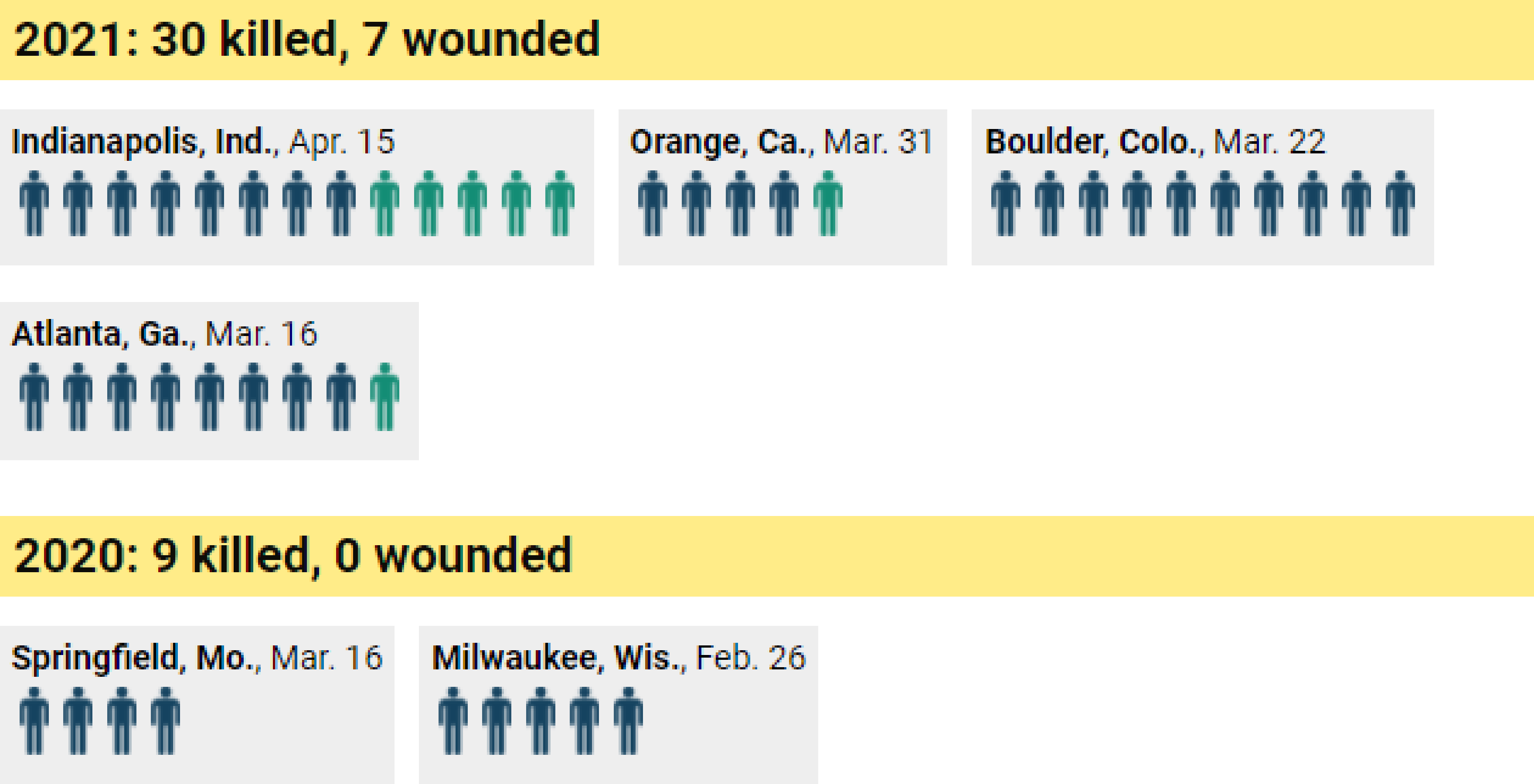
Incident Location Categories

A study of 305 Active Shooter Incidents in the U.S. between 2000 and 2019



FBI Law Enforcement Bulletin. *Active Shooter Events from 2000 to 2013, Active Shooter Incidents in the United States in 2014 and 2015, 2016 and 2017, 2018, 2019*

Mass Shootings 2020-21



2021: 30 killed, 7 wounded

Indianapolis, Ind., Apr. 15

Orange, Ca., Mar. 31

Boulder, Colo., Mar. 22

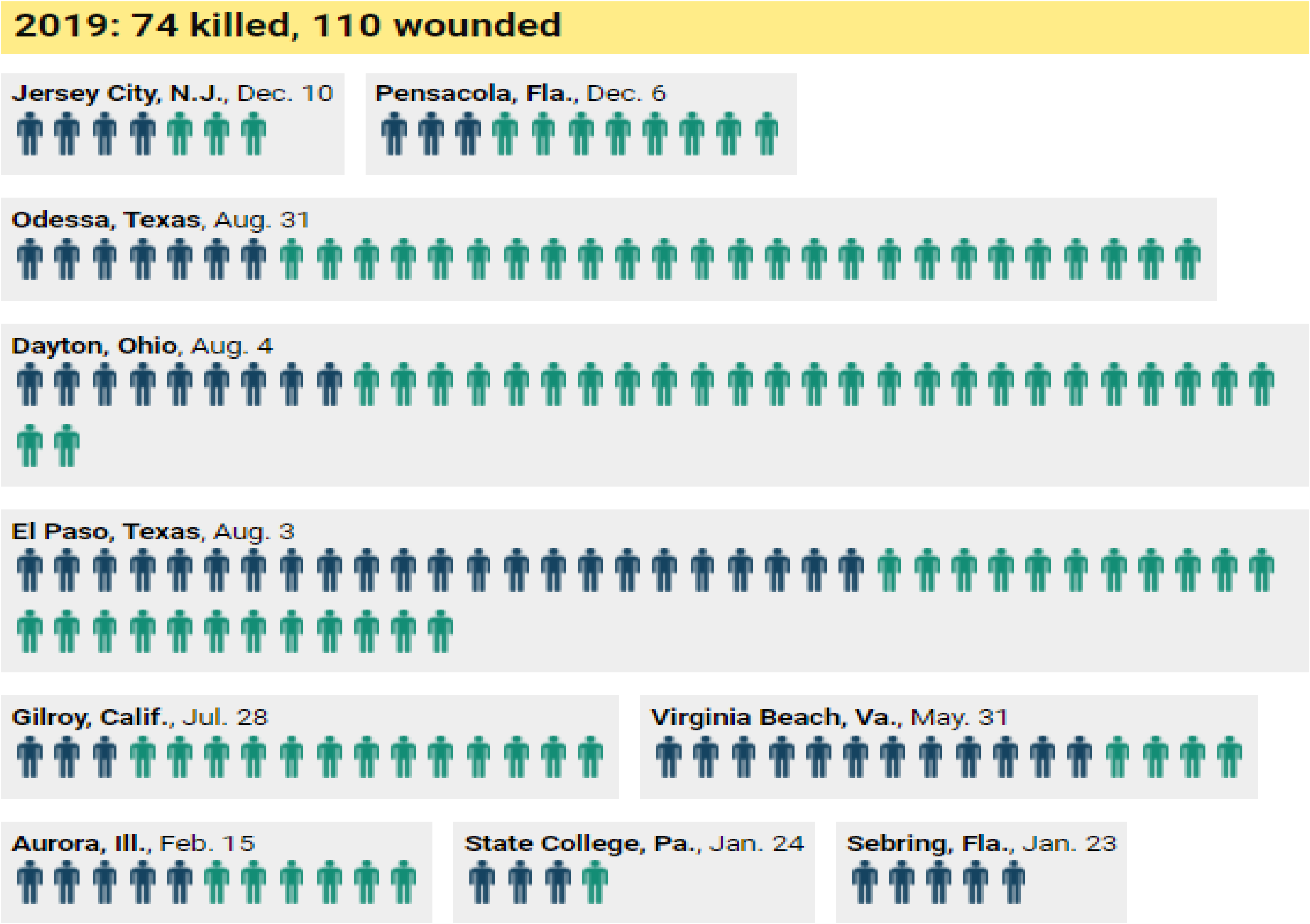
Atlanta, Ga., Mar. 16

2020: 9 killed, 0 wounded

Springfield, Mo., Mar. 16

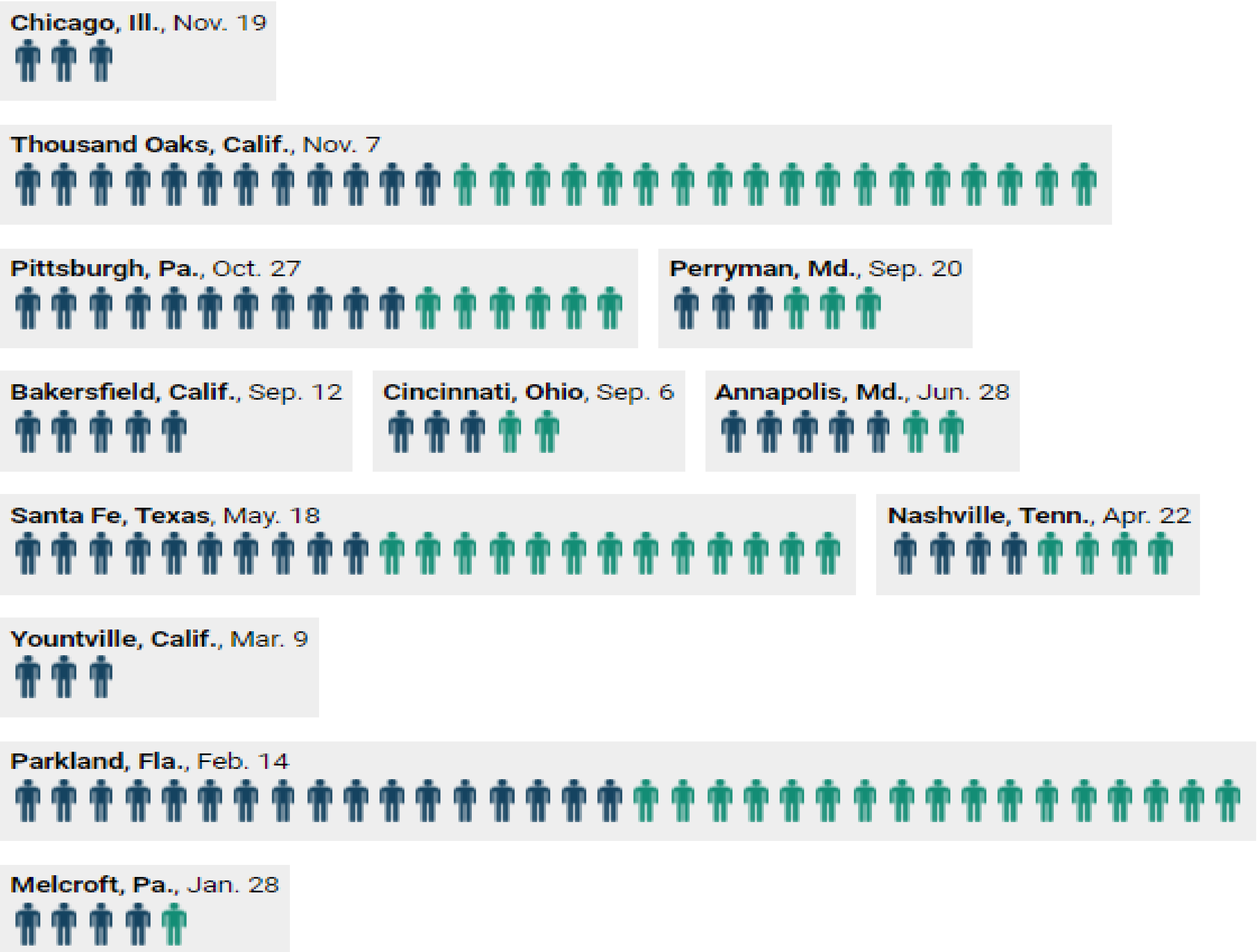
Milwaukee, Wis., Feb. 26

2019


2019: 74 killed, 110 wounded
Jersey City, N.J., Dec. 10
Pensacola, Fla., Dec. 6
Odessa, Texas, Aug. 31
Dayton, Ohio, Aug. 4
El Paso, Texas, Aug. 3
Gilroy, Calif., Jul. 28
Virginia Beach, Va., May. 31
Aurora, Ill., Feb. 15
State College, Pa., Jan. 24
Sebring, Fla., Jan. 23

2018

2018: 80 killed, 66 wounded



Chicago, Ill., Nov. 19

Thousand Oaks, Calif., Nov. 7

Pittsburgh, Pa., Oct. 27

Perryman, Md., Sep. 20

Bakersfield, Calif., Sep. 12

Cincinnati, Ohio, Sep. 6

Annapolis, Md., Jun. 28

Santa Fe, Texas, May. 18

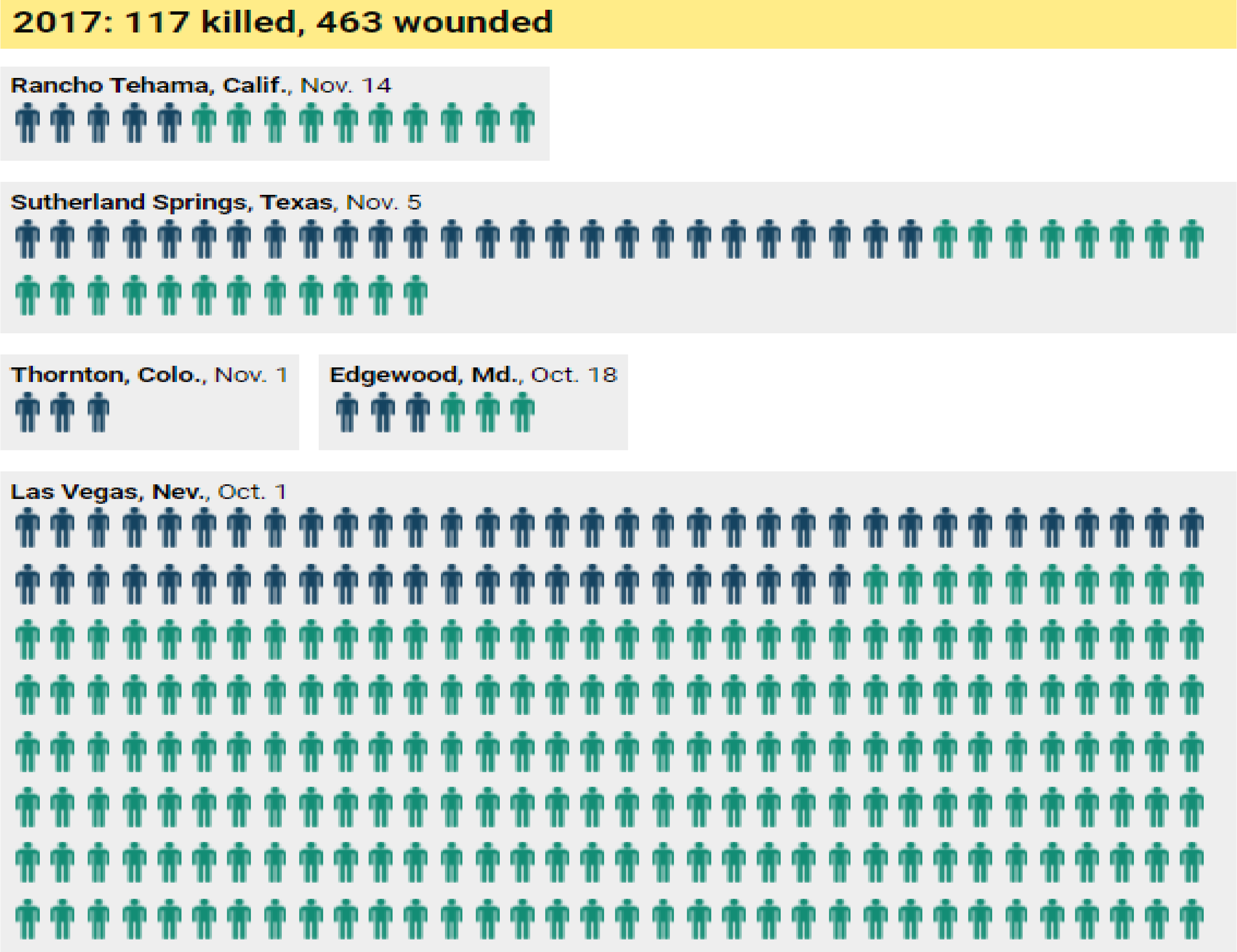
Nashville, Tenn., Apr. 22

Yountville, Calif., Mar. 9

Parkland, Fla., Feb. 14

Melcroft, Pa., Jan. 28

2017…



2017: 117 killed, 463 wounded

Rancho Tehama, Calif., Nov. 14

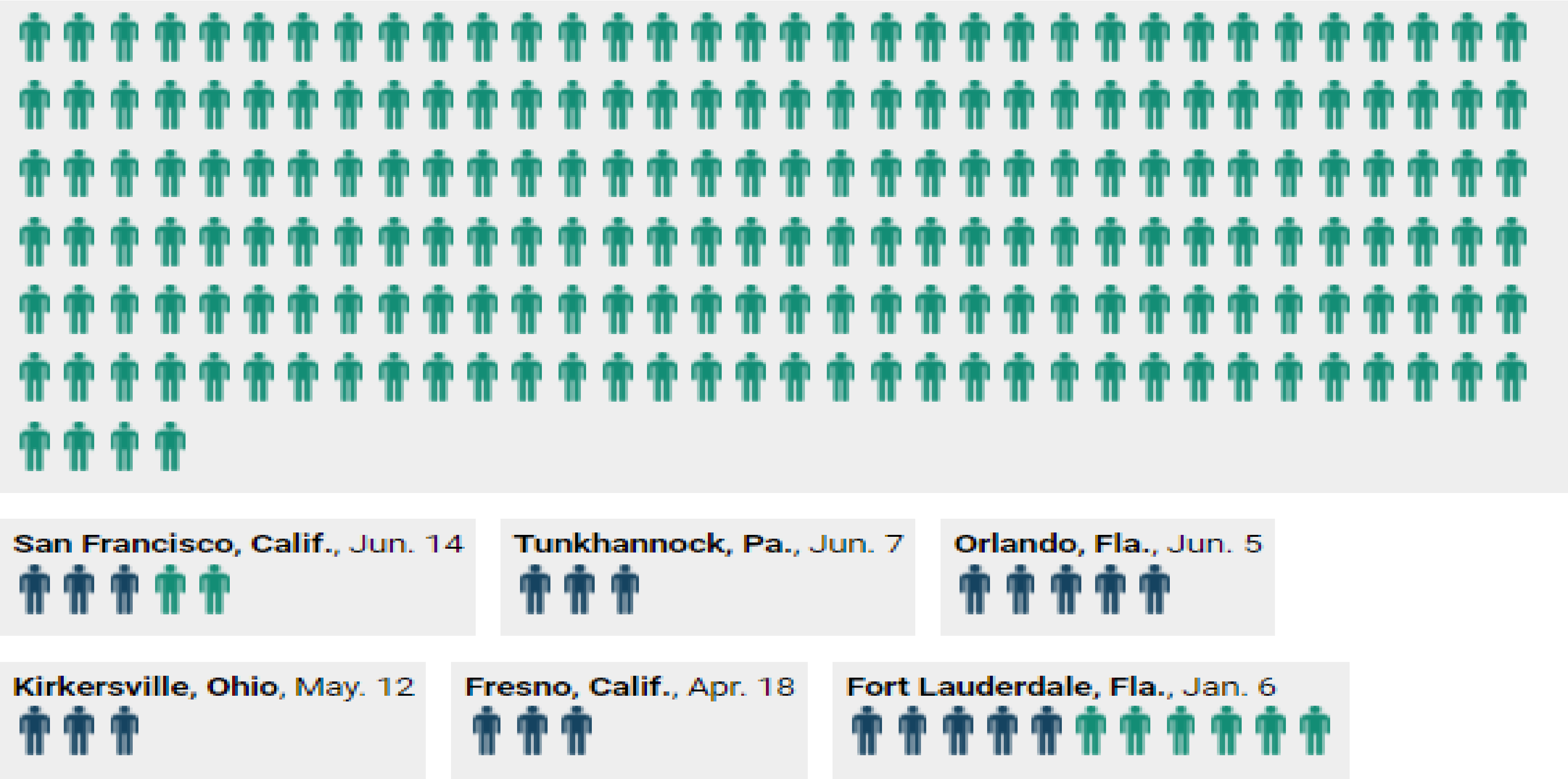
Sutherland Springs, Texas, Nov. 5

Thornton, Colo., Nov. 1

Edgewood, Md., Oct. 18

Las Vegas, Nev., Oct. 1

2017


San Francisco, Calif., Jun. 14
Tunkhannock, Pa., Jun. 7
Orlando, Fla., Jun. 5
Kirkersville, Ohio, May. 12
Fresno, Calif., Apr. 18
Fort Lauderdale, Fla., Jan. 6

Utah Incidents

2020 – Salt Lake City

Suspect pleads guilty for providing IED advice and potential targets intel to international terrorists (undercover agents)

BMM Tied to Planned Attack

2020 – South Jordan

Suspect initiates gunfire standoff from his residence. Large cache of bomb making materials found inside and detonated on site.

Investigators determine suspect was planning a targeted attack.

2019

2019 – Providence

Bombmaking in garage sends suspect to hospital.

Children in adjacent room avoid injury

Logan-based Biological Attack

2018 – Logan

Suspect charged for mailing Ricin to numerous officials, including President Trump.

Schools – Mass Gathering Venues

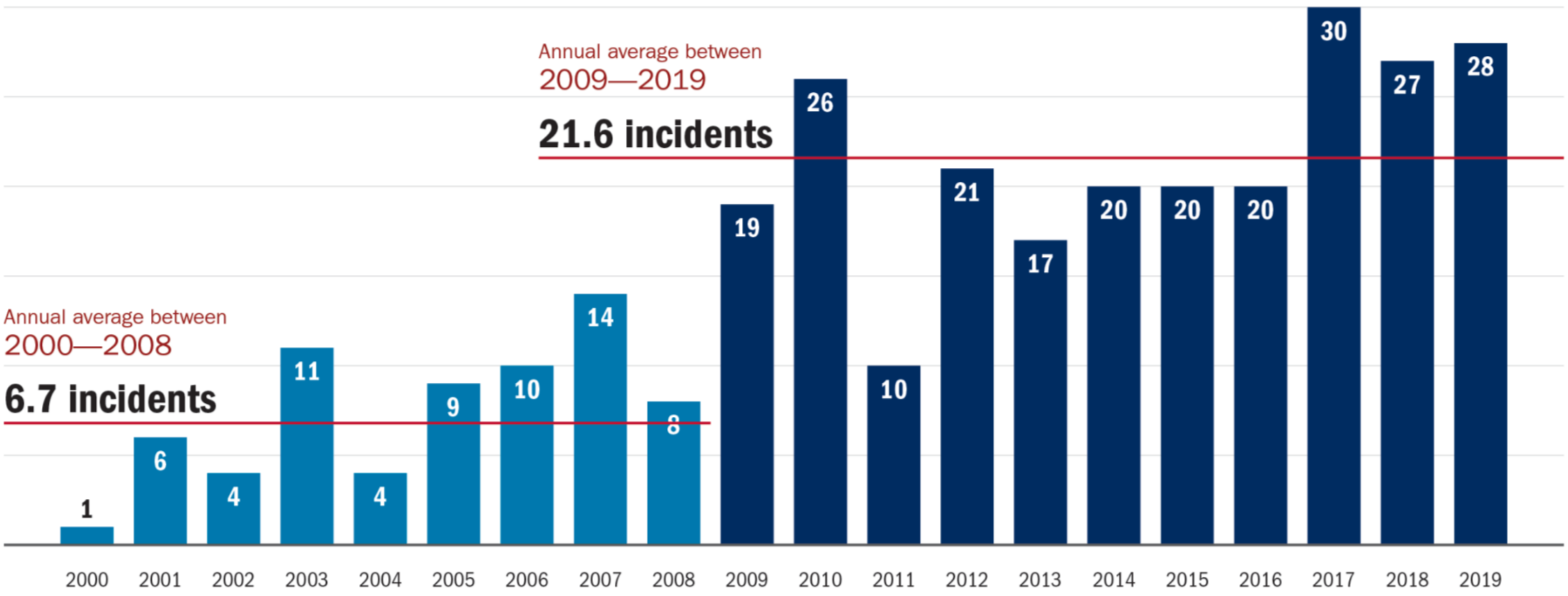
2018 - St George
16-year-old suspect attempts to detonate IED in Pineview High School cafeteria

Long history of emotional and physical bullying disclosed.

2017 – Orem
16-year-old suspect stabs five classmates and then himself. "Straight A" student with no prior indicators.

Active Shooter Trends

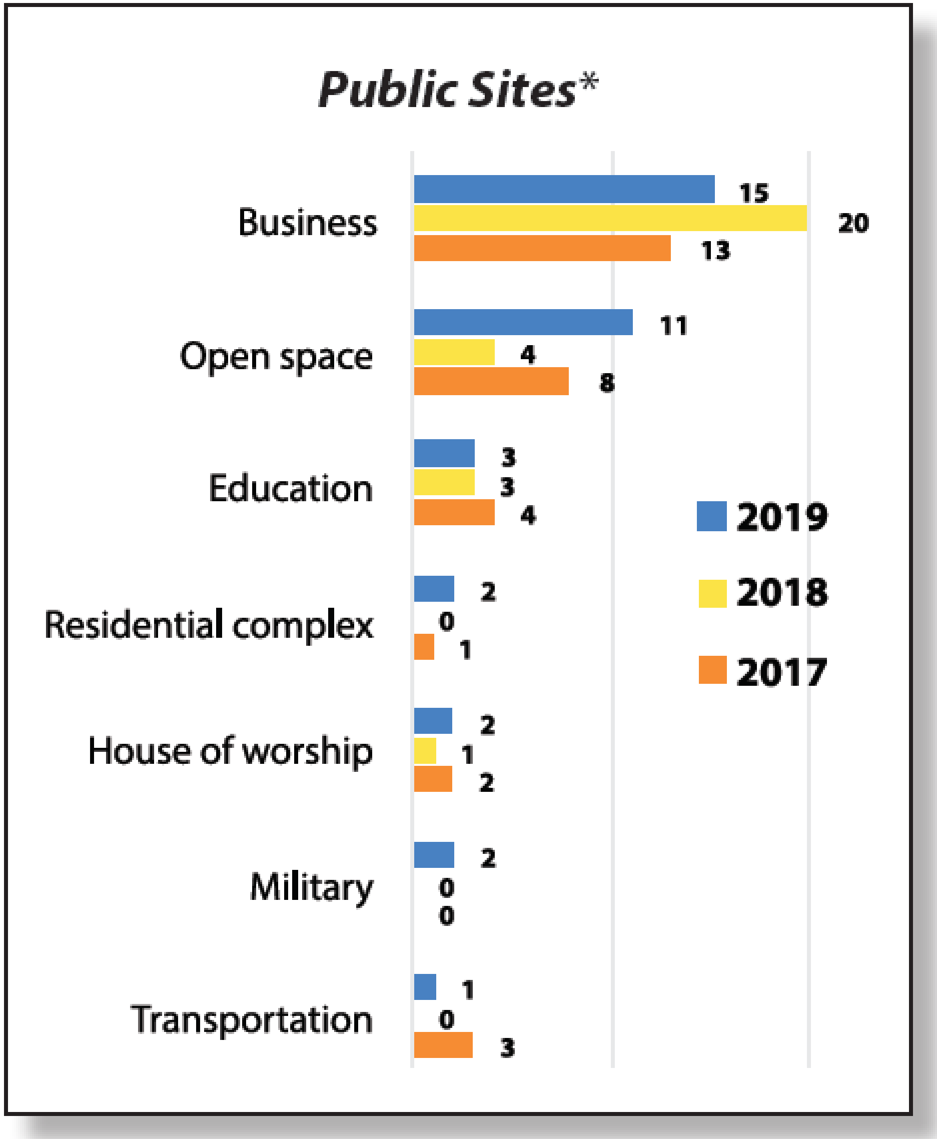
Number of Attacks Are Increasing



FBI Law Enforcement Bulletin. *Active Shooter Events from 2000 to 2013, Active Shooter Incidents in the United States in 2014, 2015, 2016 and 2017, 2018, 2019*

Soft Targets – Crowded Places

- County Fairs
- Parks - Harvest Festivals, Football & Soccer)
- Schools
- Sports stadiums
- Seats of Government
- Other Public Facilities

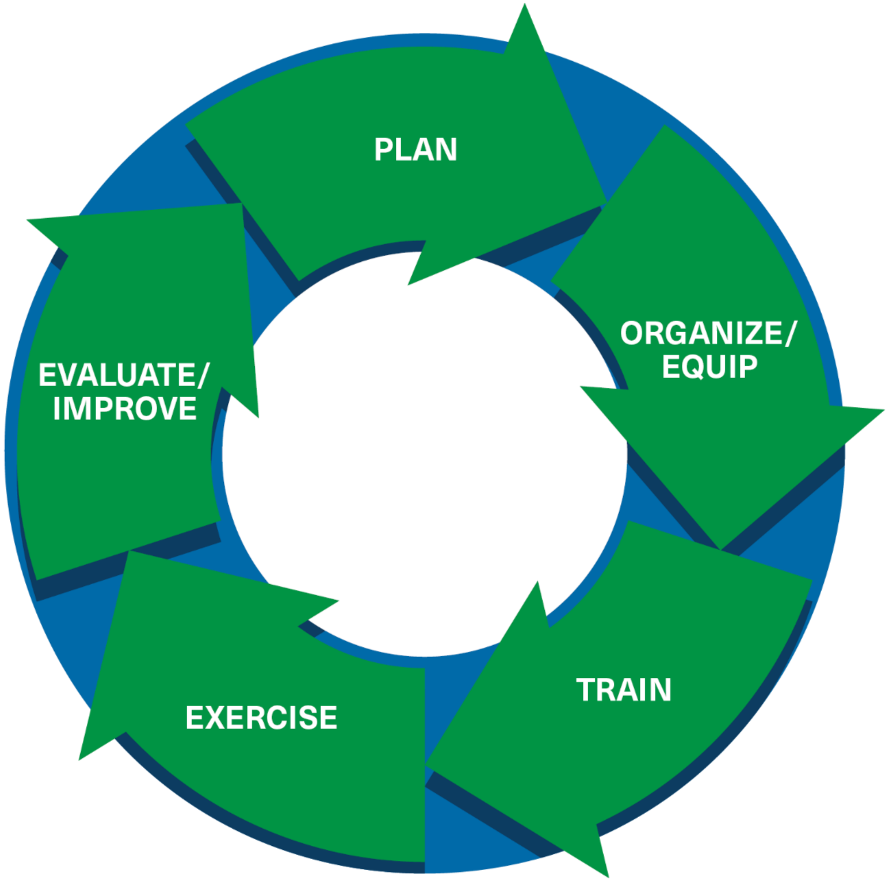


Common Public Venue Vulnerabilities

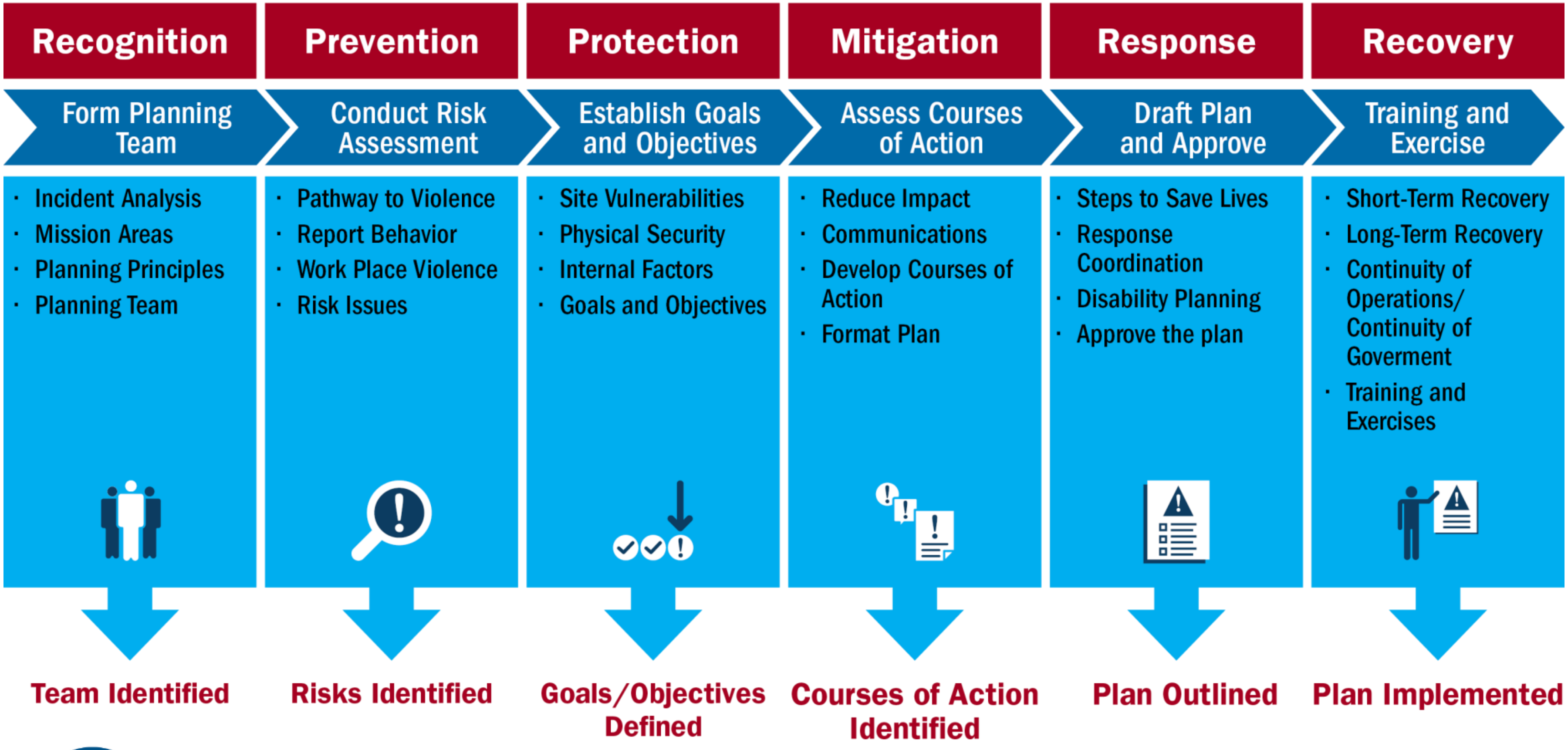
- Open Access
- Easy ingress but limited egress
- Limited security staff
- Concealed areas
- Unsecured perimeters
- Untrained staff & volunteers

Where To Start - POETEE

The Preparedness Cycle is ongoing

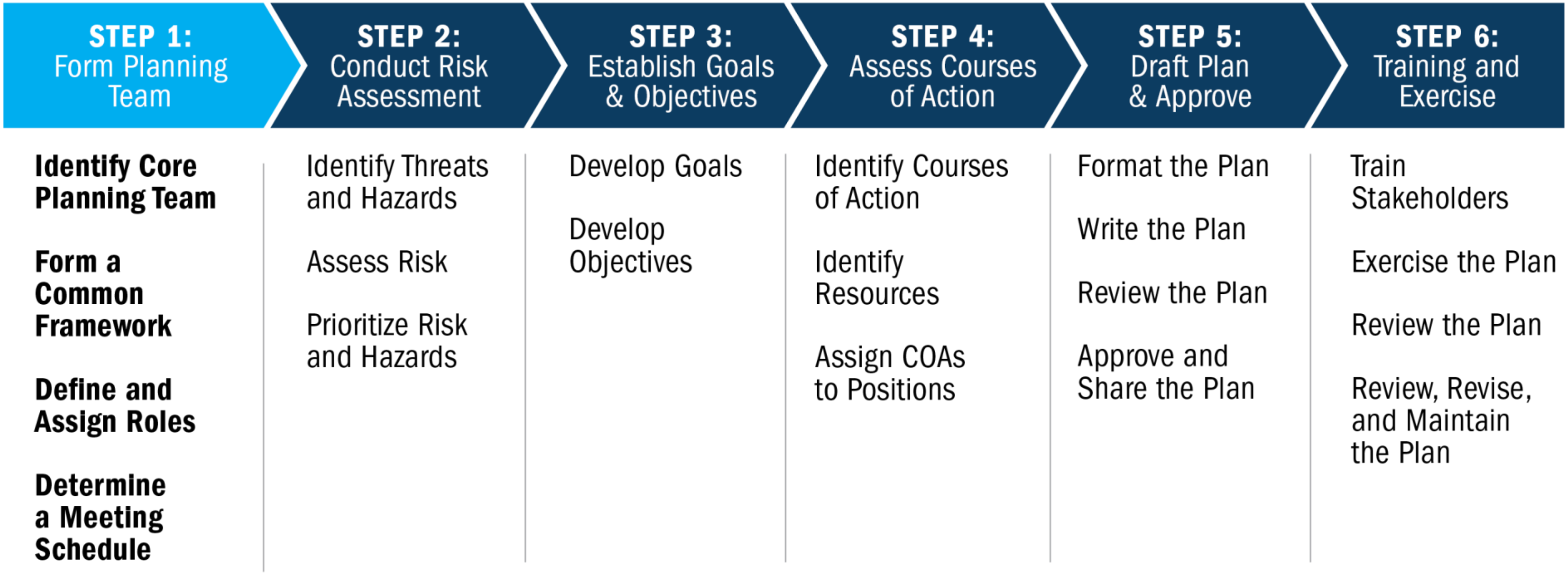


Presentation Overview



Recognition	Prevention	Protection	Mitigation	Response	Recovery
Form Planning Team	Conduct Risk Assessment	Establish Goals and Objectives	Assess Courses of Action	Draft Plan and Approve	Training and Exercise
- Incident Analysis - Mission Areas - Planning Principles - Planning Team	- Pathway to Violence - Report Behavior - Work Place Violence - Risk Issues	- Site Vulnerabilities - Physical Security - Internal Factors - Goals and Objectives	- Reduce Impact - Communications - Develop Courses of Action - Format Plan	- Steps to Save Lives - Response Coordination - Disability Planning - Approve the plan	- Short-Term Recovery - Long-Term Recovery - Continuity of Operations/ Continuity of Goverment - Training and Exercises
Team Identified	Risks Identified	Goals/Objectives Defined	Courses of Action Identified	Plan Outlined	Plan Implemented

Plan Development Steps



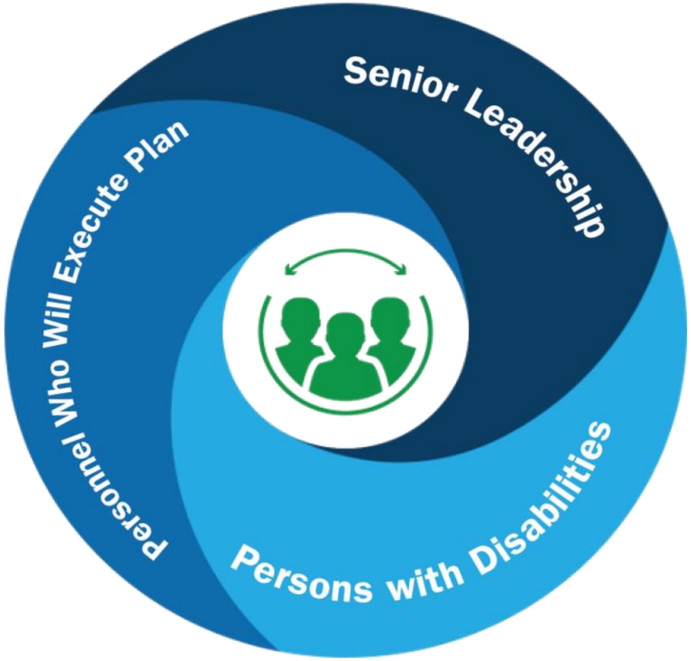
STEP 1: Form Planning Team	STEP 2: Conduct Risk Assessment	STEP 3: Establish Goals & Objectives	STEP 4: Assess Courses of Action	STEP 5: Draft Plan & Approve	STEP 6: Training and Exercise
Identify Core Planning Team **Form a Common Framework** **Define and Assign Roles** **Determine a Meeting Schedule**	Identify Threats and Hazards Assess Risk Prioritize Risk and Hazards	Develop Goals Develop Objectives	Identify Courses of Action Identify Resources Assign COAs to Positions	Format the Plan Write the Plan Review the Plan Approve and Share the Plan	Train Stakeholders Exercise the Plan Review the Plan Review, Revise, and Maintain the Plan

Form the Planning Team

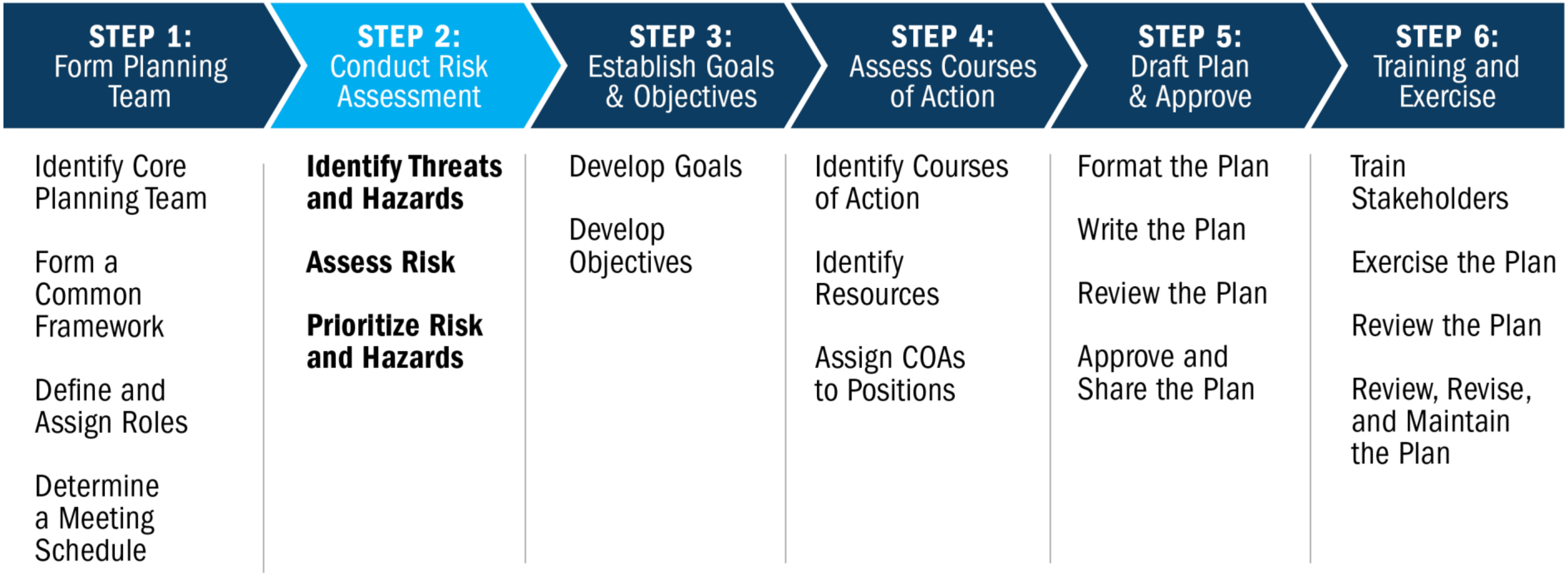
Include internal and external partners:

- Operations Managers
- Human Resources or Personnel
- Risk, Security, and Safety Directors
- General Counsel
- Maintenance or Facilities Director
- Law Enforcement, Fire, and EMS
- Landlord and Neighboring Tenants or Businesses

An effective team includes:



Step 2 in the Planning Process



STEP 1: Form Planning Team	**STEP 2:** Conduct Risk Assessment	**STEP 3:** Establish Goals & Objectives	**STEP 4:** Assess Courses of Action	**STEP 5:** Draft Plan & Approve	**STEP 6:** Training and Exercise
Identify Core Planning Team Form a Common Framework Define and Assign Roles Determine a Meeting Schedule	**Identify Threats and Hazards** **Assess Risk** **Prioritize Risk and Hazards**	Develop Goals Develop Objectives	Identify Courses of Action Identify Resources Assign COAs to Positions	Format the Plan Write the Plan Review the Plan Approve and Share the Plan	Train Stakeholders Exercise the Plan Review the Plan Review, Revise, and Maintain the Plan

Risk Analysis as a Planning Tool

Risk = potential for an unwanted outcome from an incident

R = V x T x C

Assessing risk will help you:

- Understand your situation
- Prioritize actions
- Identify and compare options
- Allocate resources

Threat and Hazard Identification and Risk Assessment Guide

Comprehensive Preparedness Guide (CPG) 201

Second Edition
August 2013

Homeland Security

Non-Disaster Grant Funding

FEMA provides funds to Utah to enhance local capabilities for dealing with terrorism, WMD, CBRNE, and cyber-based threats

- **$4.2M** State Homeland Security Program
- **$4.7M** Emergency Management Performance Grant
- **$1.4M** Non-Profit Security Grant
- Flood Mitigation Assistance
- Pre-Disaster Mitigation

Infrastructure Survey Tool - IST

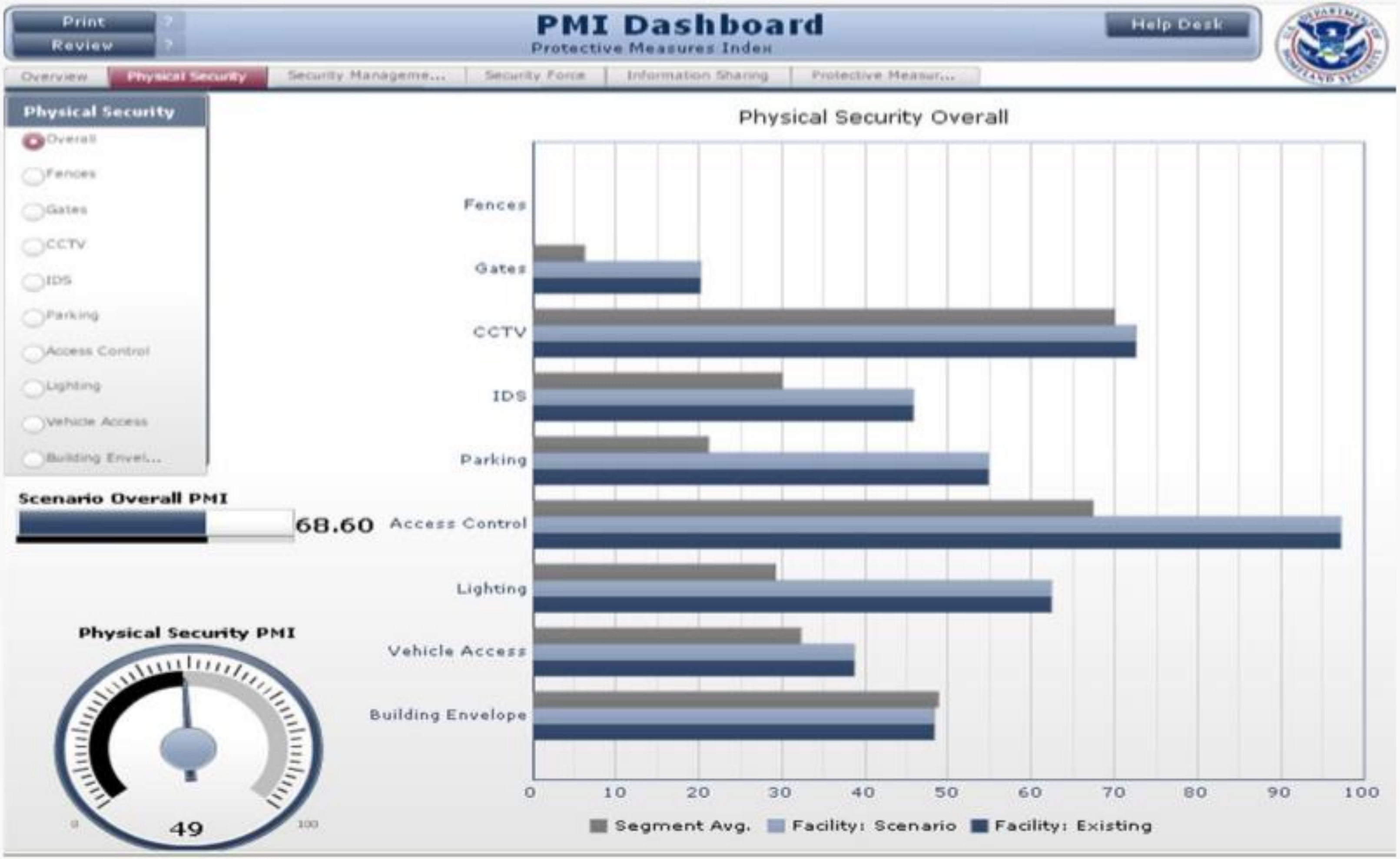
Day-long assessment focuses on

- Physical Security
- Overall resilience to disruption
- Identifies security gaps
- Provides options for closing gaps
- Provides interactive dashboard to plan and track improvements
- Encourages engagement and buy-in

IST Data Catagories

- Information sharing
- First responder relationships
- Protective measures
- Security management
- Security assets
- Security force
- Building envelope
- Vehicle access control
- Parking areas
- Delivery/loading areas
- Intrusion Detection Systems (IDS)
- CCTV surveillance
- Access controls
- Illumination
- Cybersecurity
- Physical/cyber nexus
- Dependencies (utilities)

Dashboard – Physical Security Example



Scenario Overall PMI 68.60

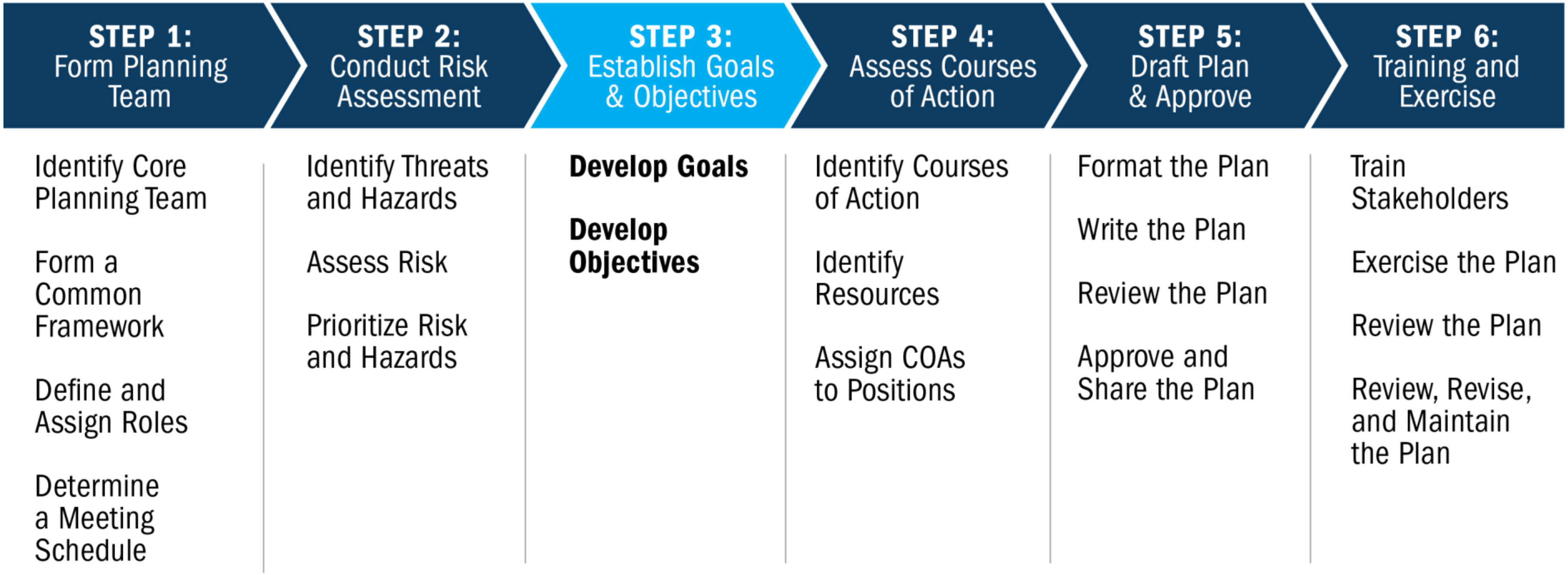
Physical Security PMI 49

Security At First Entry - SAFE

Two-hour assessment focuses on

- Information Sharing
- Communication
- Plans
- Physical Security
- Security Systems

Step 3 in the Planning Process



STEP 1: Form Planning Team	STEP 2: Conduct Risk Assessment	STEP 3: Establish Goals & Objectives	STEP 4: Assess Courses of Action	STEP 5: Draft Plan & Approve	STEP 6: Training and Exercise
Identify Core Planning Team	Identify Threats and Hazards	**Develop Goals**	Identify Courses of Action	Format the Plan	Train Stakeholders
Form a Common Framework	Assess Risk	**Develop Objectives**	Identify Resources	Write the Plan	Exercise the Plan
Define and Assign Roles	Prioritize Risk and Hazards		Assign COAs to Positions	Review the Plan	Review the Plan
Determine a Meeting Schedule				Approve and Share the Plan	Review, Revise, and Maintain the Plan

Establish Goals and Objectives

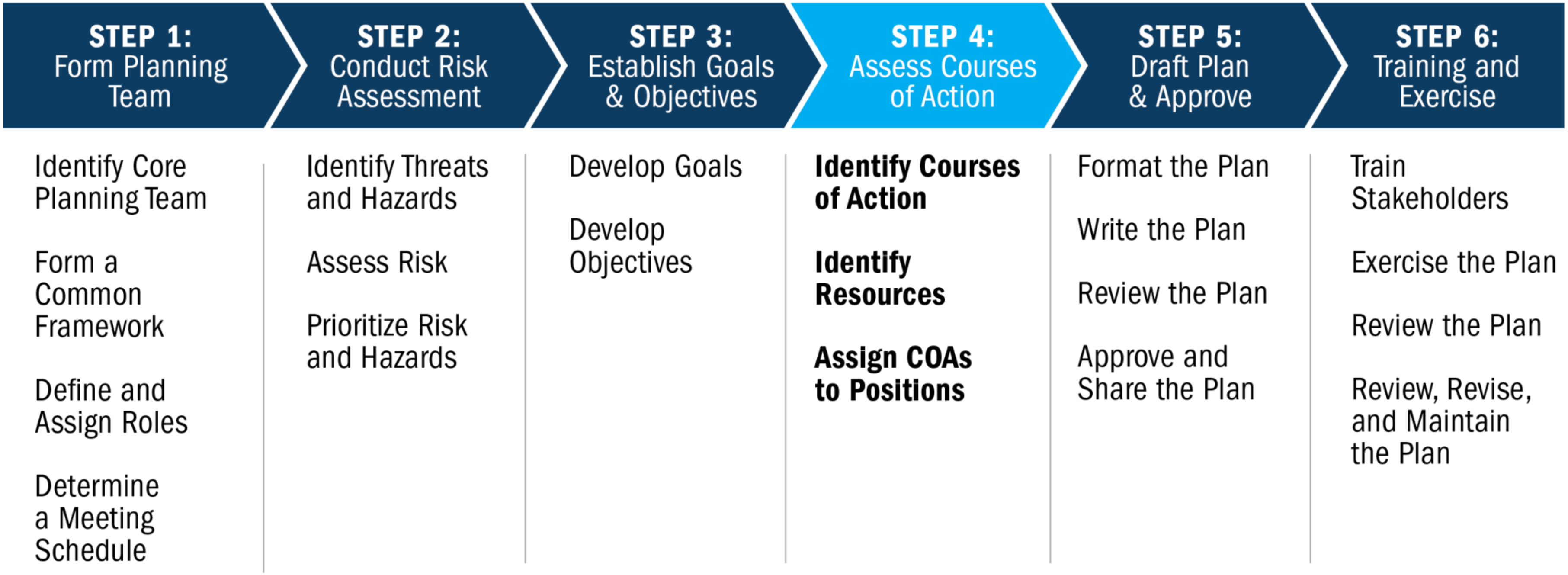
Determine Goals and Objectives

Goal: Broad statement directing personnel and resources on what they should achieve

Objective: Determining the actions participants must take in order to achieve those goals

Goals and objectives define the desired end-states for the operations addressed in the active shooter plan

Step 4 in the Planning Process



STEP 1: Form Planning Team	**STEP 2:** Conduct Risk Assessment	**STEP 3:** Establish Goals & Objectives	**STEP 4:** Assess Courses of Action	**STEP 5:** Draft Plan & Approve	**STEP 6:** Training and Exercise
Identify Core Planning Team Form a Common Framework Define and Assign Roles Determine a Meeting Schedule	Identify Threats and Hazards Assess Risk Prioritize Risk and Hazards	Develop Goals Develop Objectives	**Identify Courses of Action** **Identify Resources** **Assign COAs to Positions**	Format the Plan Write the Plan Review the Plan Approve and Share the Plan	Train Stakeholders Exercise the Plan Review the Plan Review, Revise, and Maintain the Plan

Essential Courses of Action

- Reporting
- Notification
- Evacuation
- Shelter in place
- Emergency responder coordination
- Access control
- Accountability
- Communications management
- Short-term recovery
- Long-term recovery

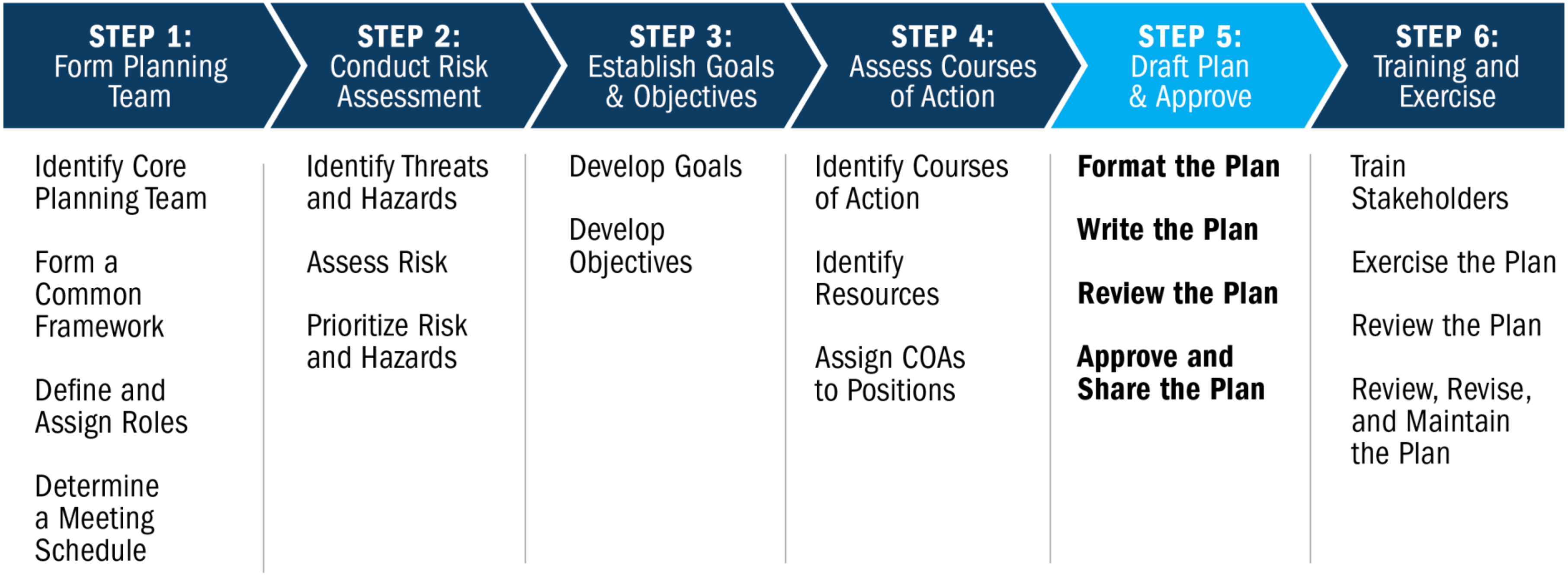
Establish Goals and Objectives

Goal: *Conduct immediate messaging or notification by all methods, including texting and computer pop-up notification.*

Objective: *Immediately initiate emergency notification including Run-Hide-Fight message via all available mediums, such as telephone, pager, email, SMS, public announcements systems, desktop/website banners, social media, etc.*

Resource: *Accessible notification software, public address system, captioning, outgoing texting through emergency notification in the area. New technologies being developed that may be applicable.*

Step 5 in the Planning Process



STEP 1:
Form Planning Team

Identify Core Planning Team

Form a Common Framework

Define and Assign Roles

Determine a Meeting Schedule

STEP 2:
Conduct Risk Assessment

Identify Threats and Hazards

Assess Risk

Prioritize Risk and Hazards

STEP 3:
Establish Goals & Objectives

Develop Goals

Develop Objectives

STEP 4:
Assess Courses of Action

Identify Courses of Action

Identify Resources

Assign COAs to Positions

STEP 5:
Draft Plan & Approve

Format the Plan

Write the Plan

Review the Plan

Approve and Share the Plan

STEP 6:
Training and Exercise

Train Stakeholders

Exercise the Plan

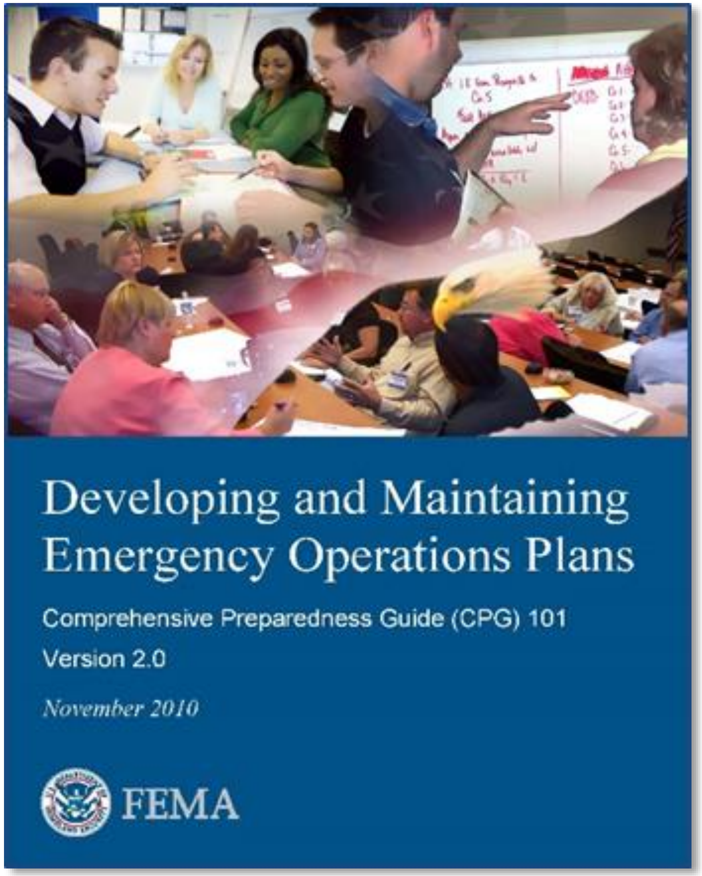
Review the Plan

Review, Revise, and Maintain the Plan

Drafting & Reviewing the Plan

Best writing practices

- Use simple language
- Use short, active voice sentences
- Give enough detail to convey easily understood, actionable guidance
- Focus on mission guidance
- Plan review criteria
- Adequacy
- Feasibility
- Acceptability
- Completeness
- Compliancy



Developing and Maintaining Emergency Operations Plans

Comprehensive Preparedness Guide (CPG) 101

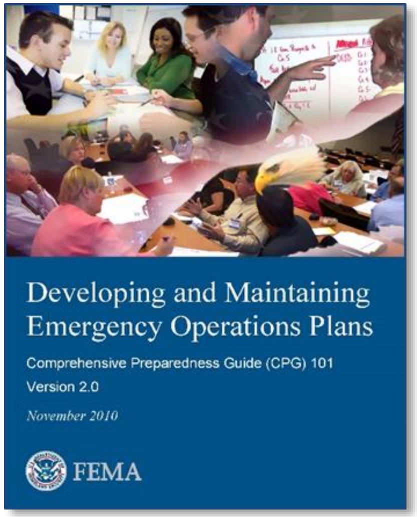
Version 2.0

November 2010

FEMA

Emergency Action Plan Resources

Whether drafting a first plan or refining an existing plan, CISA has developed the following resources to get you started:



Developing and Maintaining Emergency Operations Plans

Comprehensive Preparedness Guide (CPG) 101

Version 2.0

November 2010

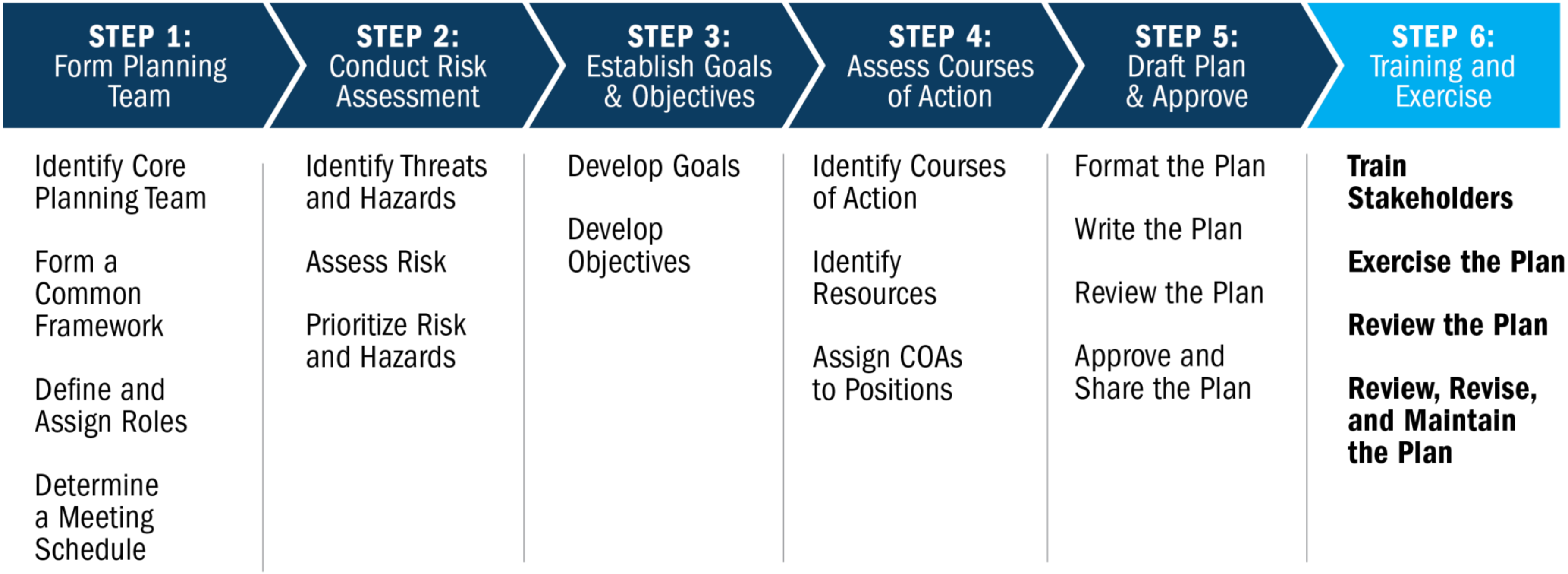
FEMA

The **Active Shooter Emergency Plan Guide** is a virtual learning tool that helps organizations take the first steps toward building an EAP. cisa.gov/sites/default/files/publications/active-shooter-emergency-action-plan-112017-508v2.pdf

The **Active Shooter Emergency Action Plan Template** is a fillable form to document the organization’s EAP. cisa.gov/sites/default/files/publications/active-shooter-emergency-action-plan-template-112017-508.pdf

The **Active Shooter Emergency Action Plan Video** uses first-hand perspectives of those who have survived incidents to inform and guide developers of EAPs. cisa.gov/active-shooter-emergency-action-plan-video

Step 6 in the Planning Process



STEP 1: Form Planning Team

- Identify Core Planning Team
- Form a Common Framework
- Define and Assign Roles
- Determine a Meeting Schedule

STEP 2: Conduct Risk Assessment

- Identify Threats and Hazards
- Assess Risk
- Prioritize Risk and Hazards

STEP 3: Establish Goals & Objectives

- Develop Goals
- Develop Objectives

STEP 4: Assess Courses of Action

- Identify Courses of Action
- Identify Resources
- Assign COAs to Positions

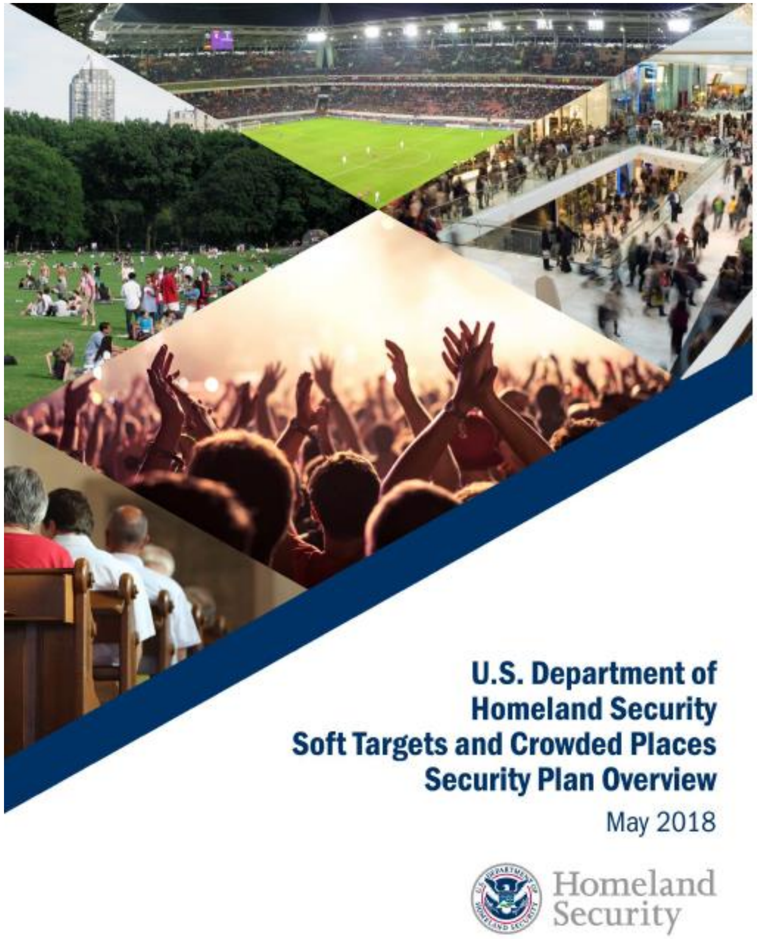
STEP 5: Draft Plan & Approve

- Format the Plan
- Write the Plan
- Review the Plan
- Approve and Share the Plan

STEP 6: Training and Exercise

- **Train Stakeholders**
- **Exercise the Plan**
- **Review the Plan**
- **Review, Revise, and Maintain the Plan**

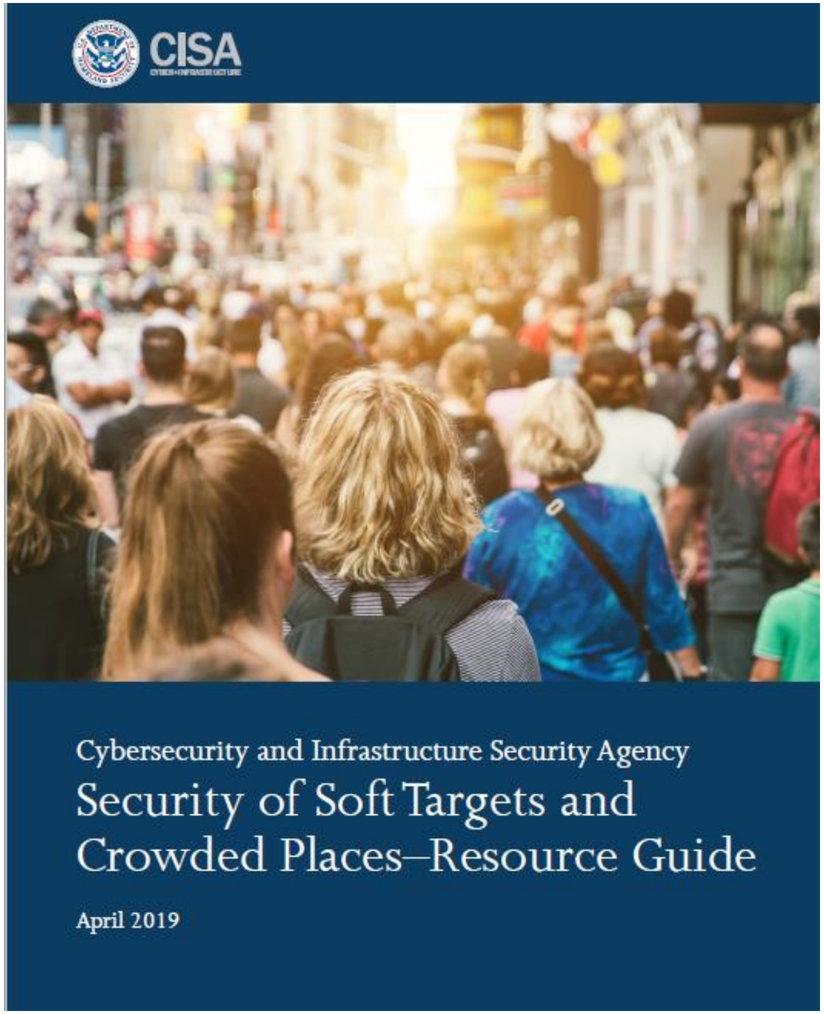
Additional Planning Resources



U.S. Department of
Homeland Security
Soft Targets and Crowded Places
Security Plan Overview

May 2018

Homeland
Security



CISA

Cybersecurity and Infrastructure Security Agency

Security of Soft Targets and
Crowded Places–Resource Guide

April 2019

cisa.gov/securing-public-gatherings

- All Stakeholders
- Businesses and Critical Infrastructure
- SLTT Authorities, Government, First Responders
- Schools
- Houses of Worship

First Preventers

- Prevent targeted violence
- Train employees to recognize behaviors on the **pathway to violence.**
- Instill a positive culture for reporting.
- Develop intervention capabilities.

Awareness + Action = Prevention

Workplace Violence and Categories

TYPE 1

Violent acts by criminals who have no other connection with the workplace but enter to commit robbery or another crime.

TYPE 2

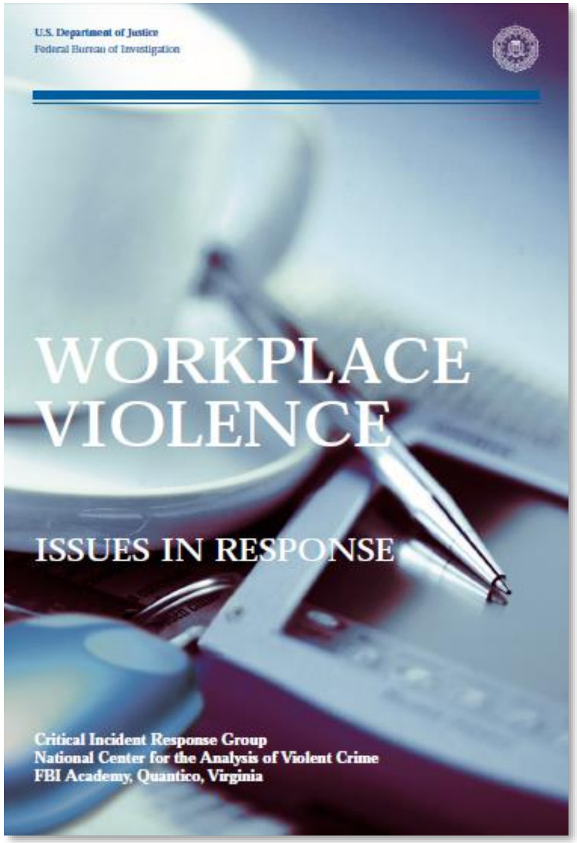
Violence directed at employees by customers, clients, patients, students, inmates, or any others for whom an organization provides services.

TYPE 3

Violence against coworkers, supervisors, or managers by a present or former employee.

TYPE 4

Violence committed in the workplace by someone who doesn’t work there, but has a personal relationship with an employee—an abusive spouse or domestic partner.



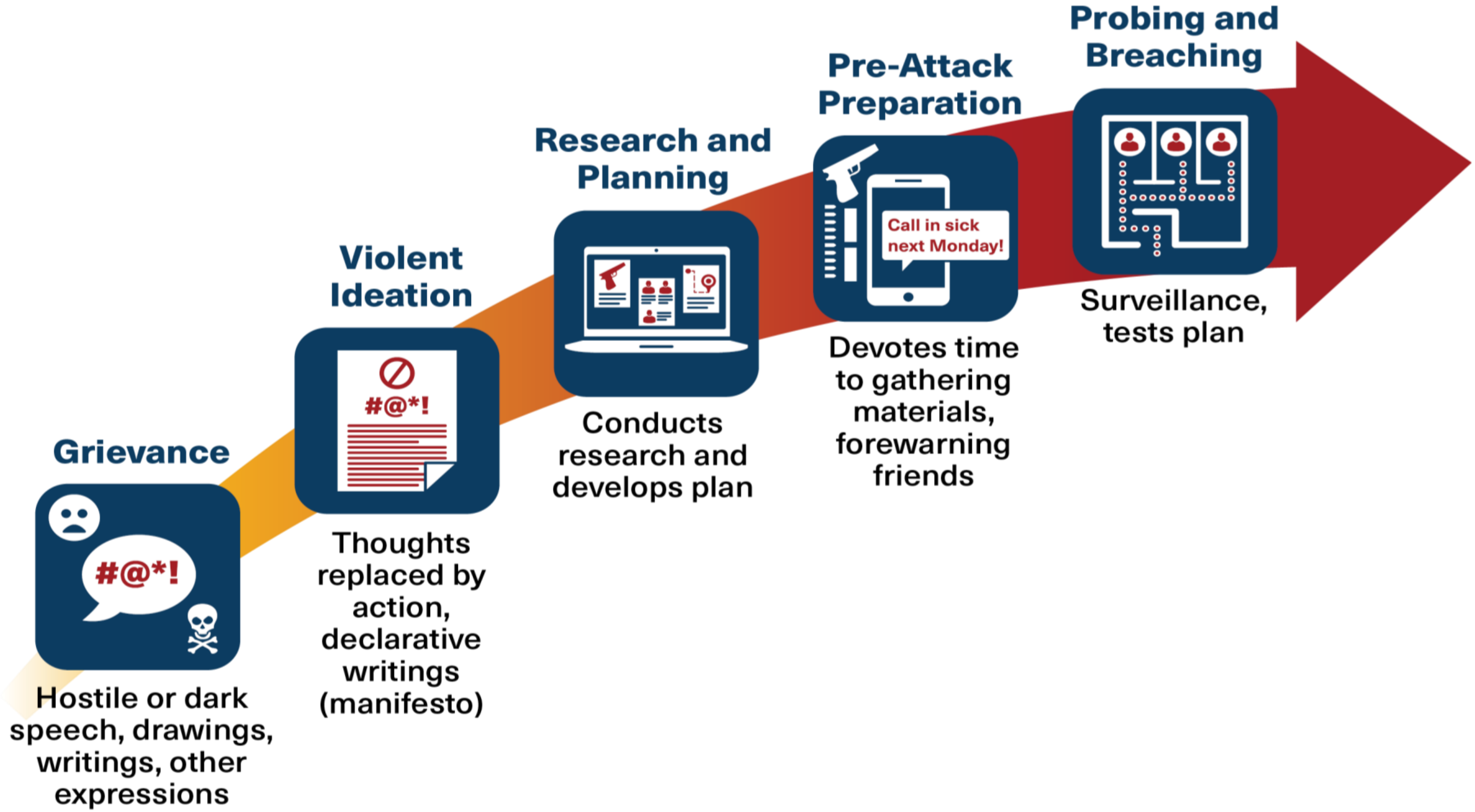
U.S. Department of Justice
Federal Bureau of Investigation

WORKPLACE VIOLENCE

ISSUES IN RESPONSE

Critical Incident Response Group
National Center for the Analysis of Violent Crime
FBI Academy, Quantico, Virginia

Pathway to Violence



Grievance

Hostile or dark speech, drawings, writings, other expressions

Violent Ideation

Thoughts replaced by action, declarative writings (manifesto)

Research and Planning

Conducts research and develops plan

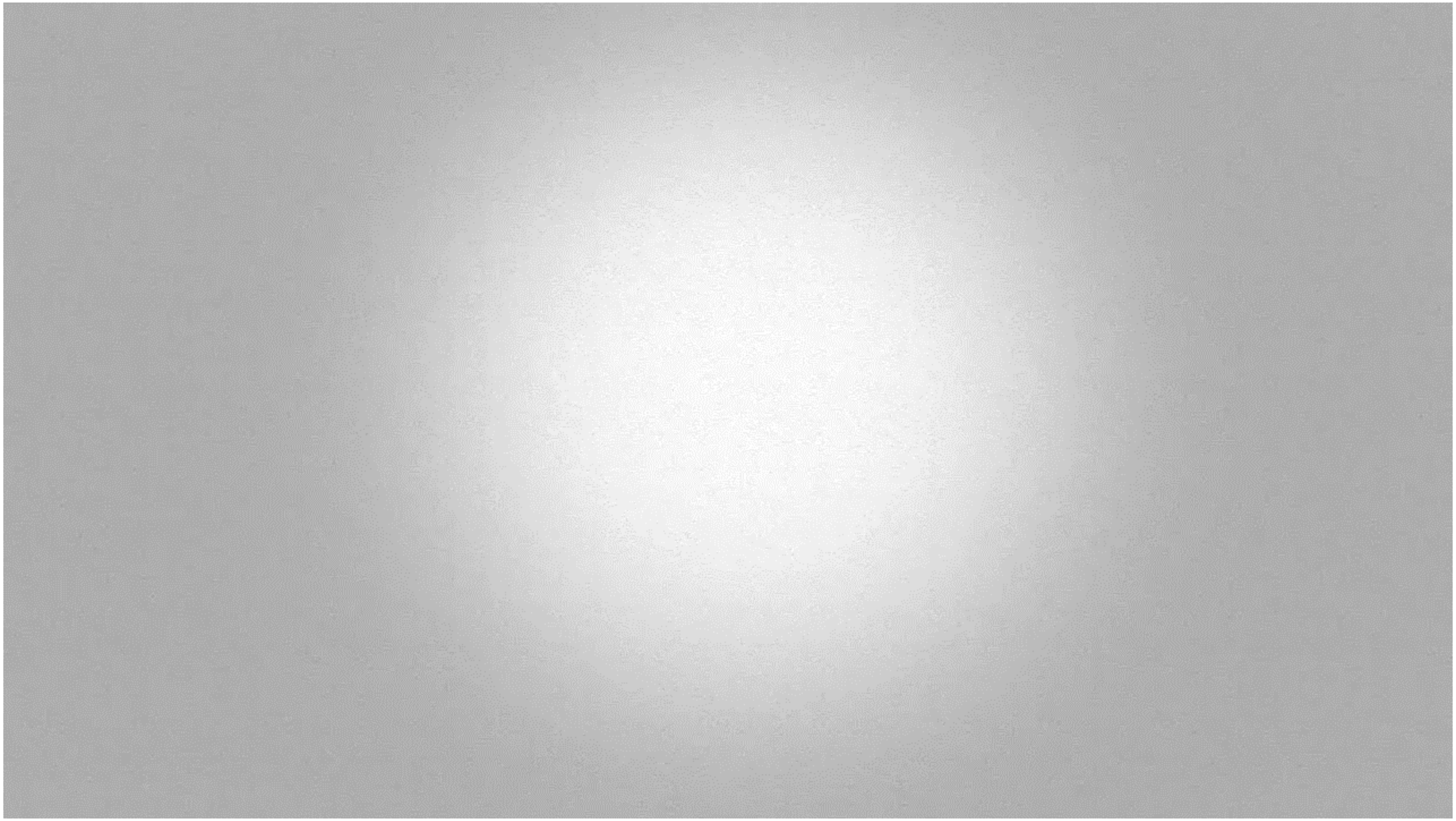
Pre-Attack Preparation

Devotes time to gathering materials, forewarning friends

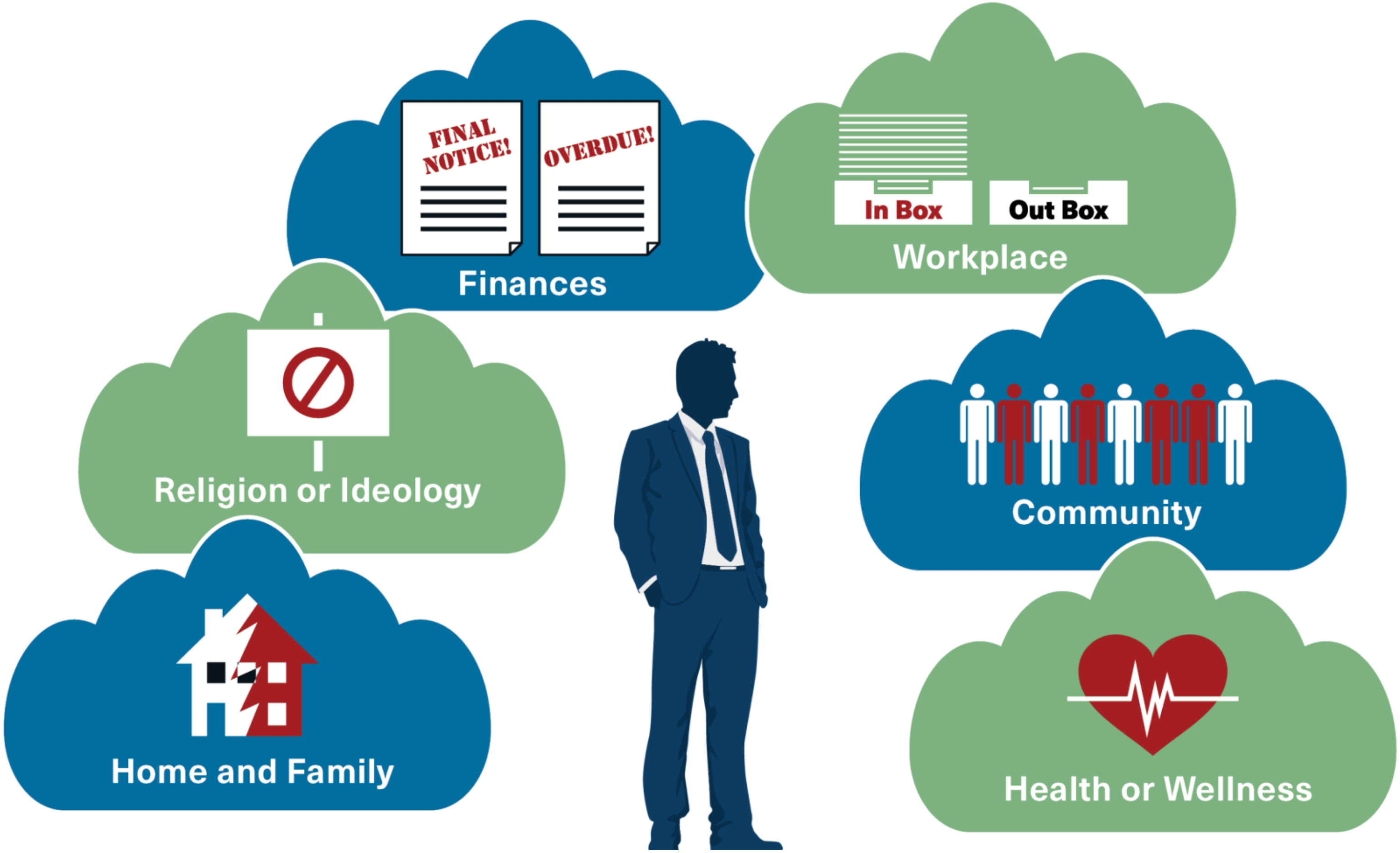
Probing and Breaching

Surveillance, tests plan

Video: Pathway to Violence



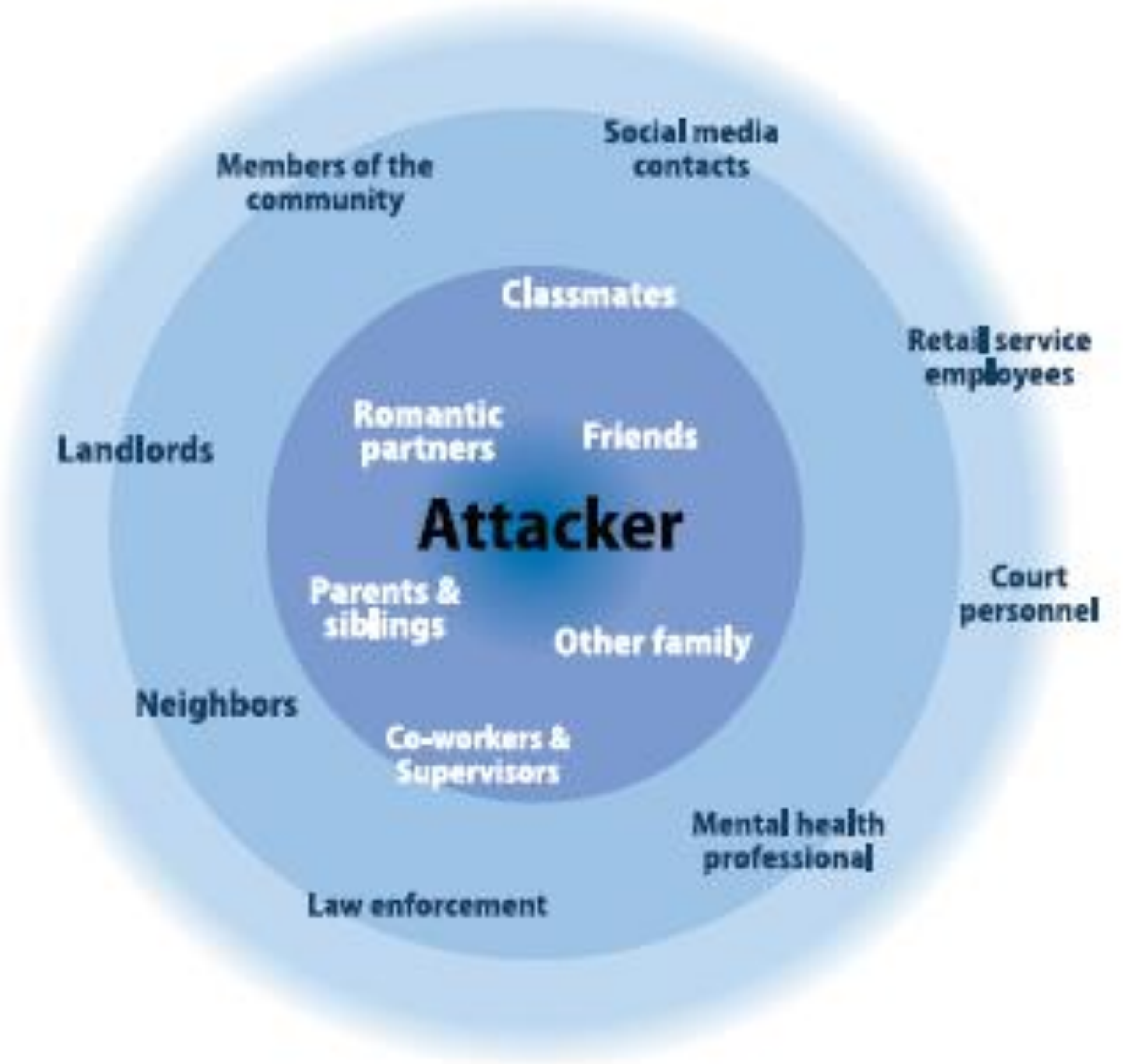
Behavioral Change Initiators



Behavioral Indicators

Speech

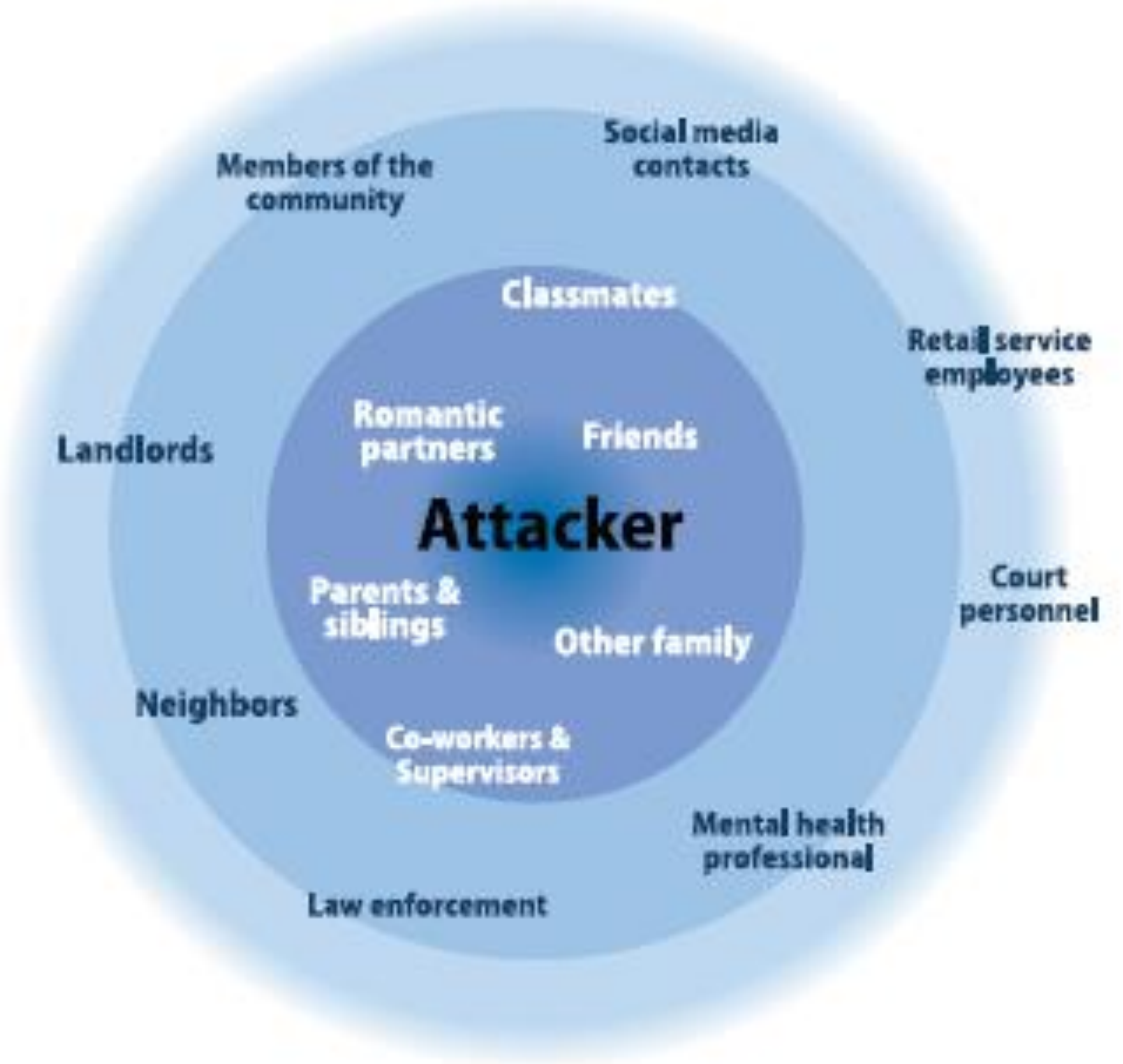
- Expression of suicidal tendencies
- Talking about previous violent incidents
- Unsolicited focus on dangerous weapons
- Paranoid thinking
- Overreaction to workplace changes



Behavioral Indicators

Feelings

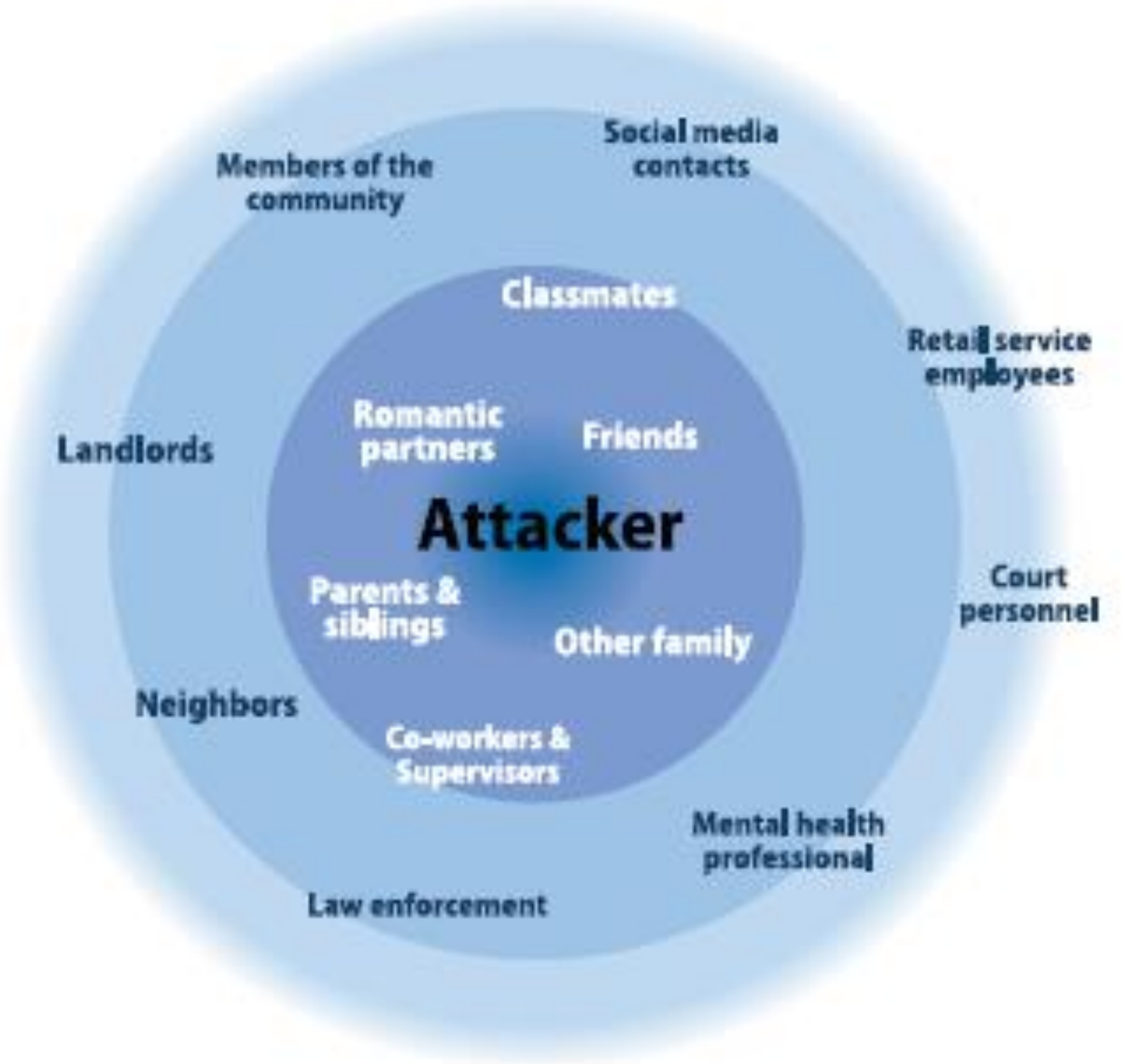
- Depression or withdrawal
- Unstable, emotional responses
- Feeling either arrogant and supreme or powerless
- Intense anger or hostility



Behavioral Indicators

Behaviors

- Increased use of alcohol or drugs
- Violations of company policies
- Increased absenteeism
- Exploiting or blaming others



Threat Assessment

- ✓ Identify behaviors to enable early intervention
- ✓ Notice an increase in intensity or “red flags”
- ✓ Threat Assessment Teams conduct evaluations
- ✓ Ongoing outreach and engagement

Threat Management Team

- Your team should align to company culture, structure, business, and characteristics
- Ensure a multi-disciplinary approach

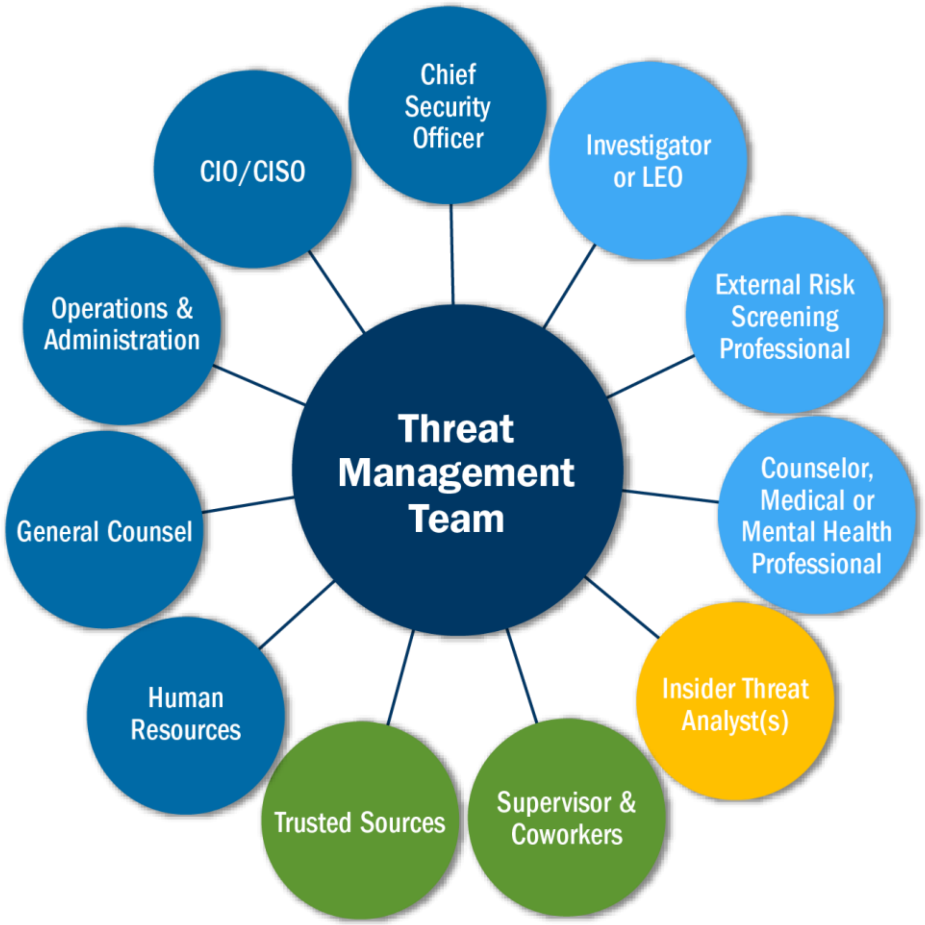
Leverage organic and existing functions

Involve external resources on case-by-case basis

Gather information from trusted sources

For some entities of sufficient size, complexity, or risk, consider dedicated resources

- The "truth is out there" and can be ascertained through inclusion and before a totality assessment



Intervention

Consider a range of passive and active strategies geared toward preventing insider threat actions

- Take no action
- Watch and wait
- Employee Assistance Program referral
- Drug and alcohol testing
- Performance assessment
- Medical attention or counseling
- Third party monitoring
- Interview with supervisor and coworkers
- Direct interview

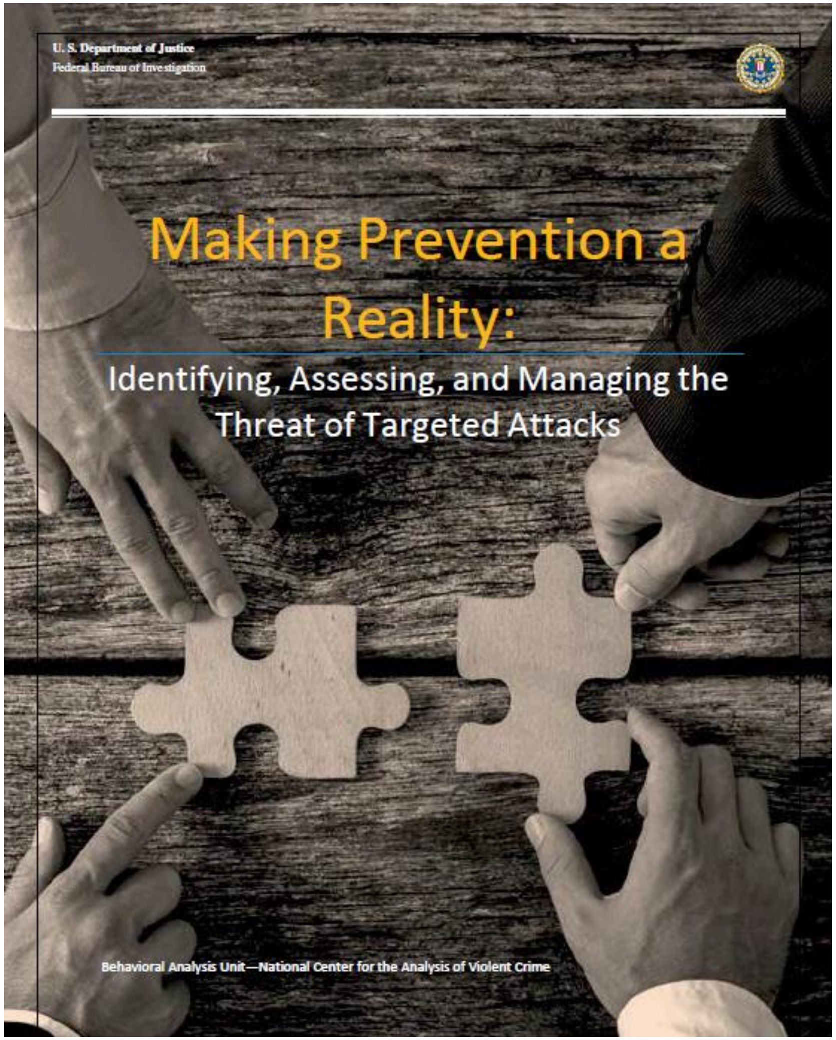
- Monitoring and investigating – employee records, social media, computer/network activity
- Physical/information security measures
- Violence risk assessment
- Target risk reduction
- Administrative actions – disciplinary leave, reassignment, safe termination
- Law enforcement involvement
- Legal actions (civil or criminal)

Threat Management Teams

Viable strategies to reduce targeted violence

- Identify
- Assess
- Manage

Prevention is not a passive process



U. S. Department of Justice
Federal Bureau of Investigation

Making Prevention a Reality:

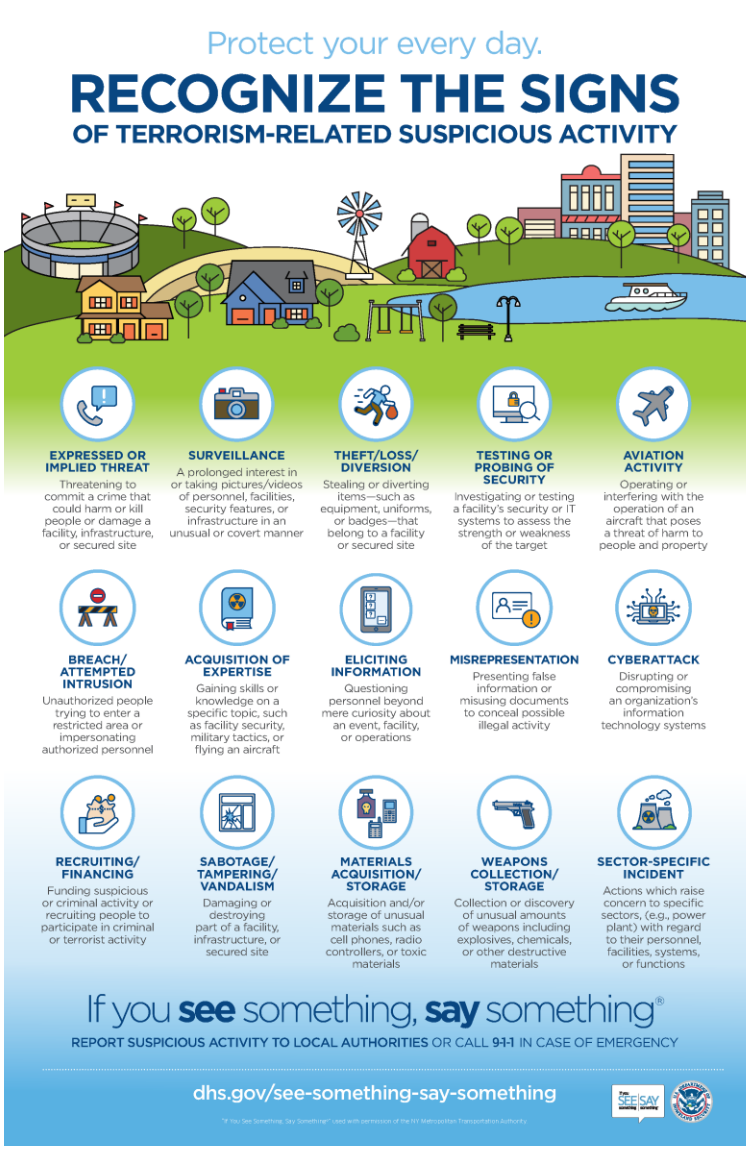
Identifying, Assessing, and Managing the Threat of Targeted Attacks

Behavioral Analysis Unit—National Center for the Analysis of Violent Crime

First Preventers

- **See Something / Say Something**
- Train employees to recognize behaviors on the **pathway to violence.**
- Instill a positive culture for reporting.
- Develop intervention capabilities.

Awareness + Action = Prevention



Protect your every day.

RECOGNIZE THE SIGNS

OF TERRORISM-RELATED SUSPICIOUS ACTIVITY

EXPRESSED OR IMPLIED THREAT
Threatening to commit a crime that could harm or kill people or damage a facility, infrastructure, or secured site

SURVEILLANCE
A prolonged interest in or taking pictures/videos of personnel, facilities, security features, or infrastructure in an unusual or covert manner

THEFT/LOSS/ DIVERSION
Stealing or diverting items—such as equipment, uniforms, or badges—that belong to a facility or secured site

TESTING OR PROBING OF SECURITY
Investigating or testing a facility's security or IT systems to assess the strength or weakness of the target

AVIATION ACTIVITY
Operating or interfering with the operation of an aircraft that poses a threat of harm to people and property

BREACH/ ATTEMPTED INTRUSION
Unauthorized people trying to enter a restricted area or impersonating authorized personnel

ACQUISITION OF EXPERTISE
Gaining skills or knowledge on a specific topic, such as facility security, military tactics, or flying an aircraft

ELICITING INFORMATION
Questioning personnel beyond mere curiosity about an event, facility, or operations

MISREPRESENTATION
Presenting false information or misusing documents to conceal possible illegal activity

CYBERATTACK
Disrupting or compromising an organization's information technology systems

RECRUITING/ FINANCING
Funding suspicious or criminal activity or recruiting people to participate in criminal or terrorist activity

SABOTAGE/ TAMPERING/ VANDALISM
Damaging or destroying part of a facility, infrastructure, or secured site

MATERIALS ACQUISITION/ STORAGE
Acquisition and/or storage of unusual materials such as cell phones, radio controllers, or toxic materials

WEAPONS COLLECTION/ STORAGE
Collection or discovery of unusual amounts of weapons including explosives, chemicals, or other destructive materials

SECTOR-SPECIFIC INCIDENT
Actions which raise concern to specific sectors, (e.g., power plant) with regard to their personnel, facilities, systems, or functions

If you **see** something, **say** something®

REPORT SUSPICIOUS ACTIVITY TO LOCAL AUTHORITIES OR CALL **9-1-1** IN CASE OF EMERGENCY

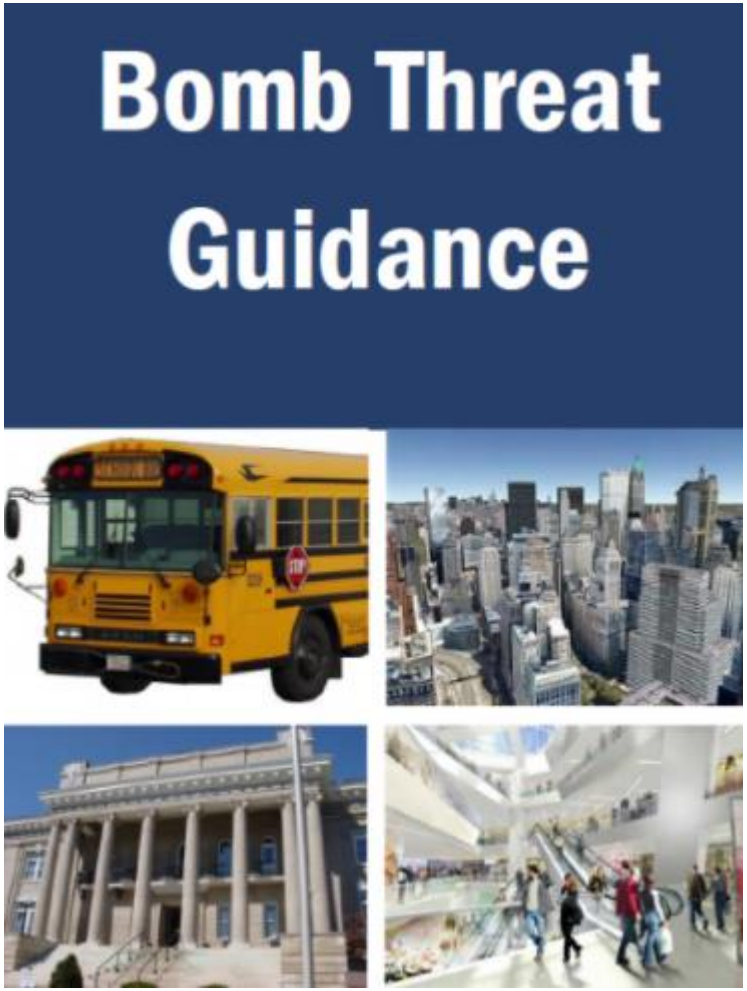
dhs.gov/see-something-say-something

"If You See Something, Say Something®" used with permission of the NY Metropolitan Transportation Authority.

First Preventers

- **React to a bomb threat in an orderly and controlled manner**
- Pre-threat preparation
- Threat assessment considerations
- Staff response guidelines
- Evacuation and shelter-in-place considerations

Awareness + Action = Prevention



Bomb Threat Guidance

Mitigation - Layered Security

- **Deter**
- **Detect**
- **Delay**
- **Defend**

Make investments that improve security over time

Mitigation Considerations

Mitigation incorporates a multi-disciplinary approach to deter active shooter incidents.

Assessment of risk and vulnerabilities

Identifying best practices for active shooter mitigation

Implementing steps to mitigate

Mitigation Actions

Establish

Identify-Assess -Manage Processes

Procedures

Practice immediate action drills

Plan

Designate shelter locations

Training

Mandatory **Run–Hide–Fight** training

Systems

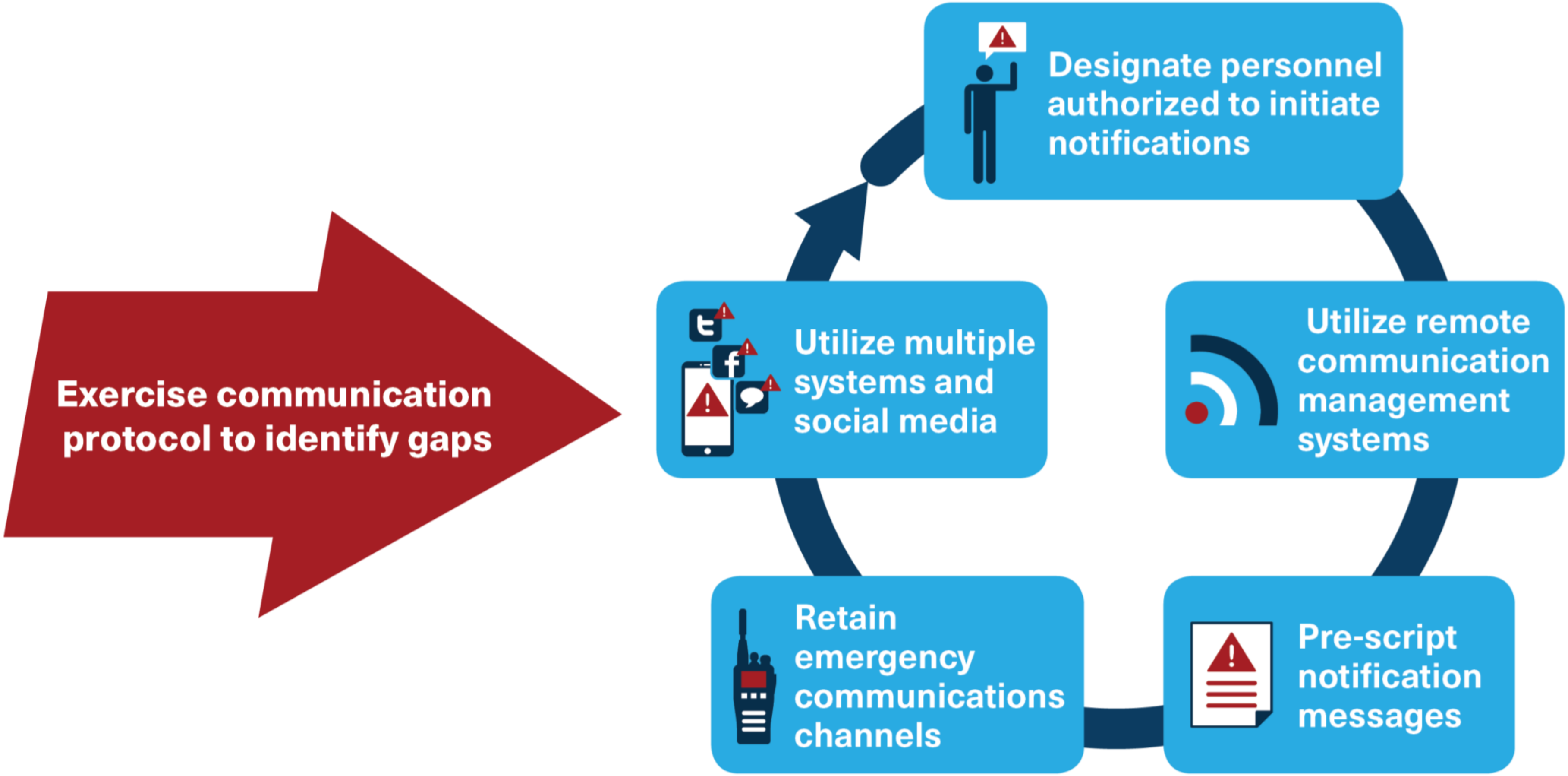
Access control, video monitoring system

Coordination

Integrate with responder agencies

Immediate notification to all occupants and visitors of an active shooter incident is a critical mitigation action.

Mitigation - Notification



Exercise communication protocol to identify gaps

Designate personnel authorized to initiate notifications

Utilize remote communication management systems

Pre-script notification messages

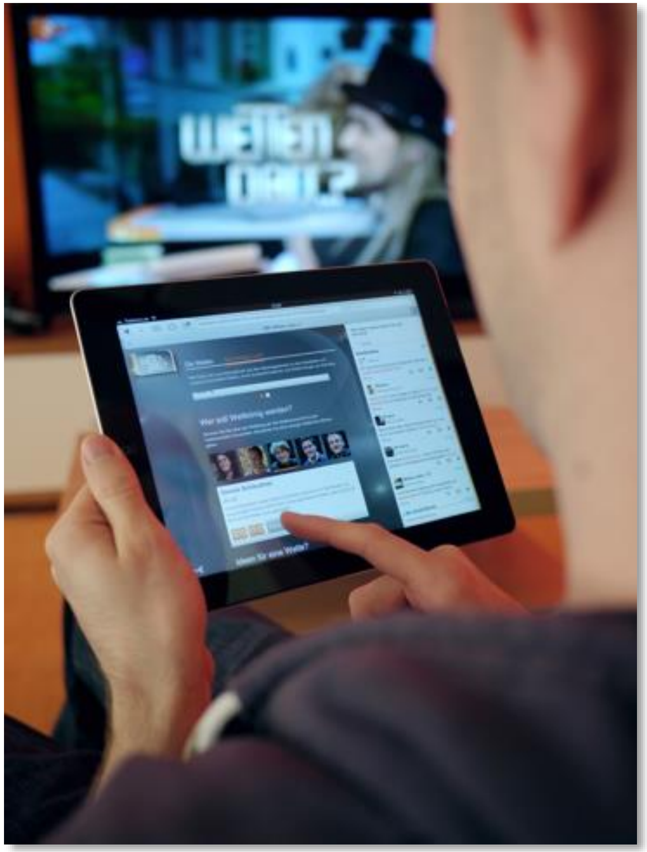
Retain emergency communications channels

Utilize multiple systems and social media

Notification Considerations

Effective Communication Platforms

- IMMEDIATE, clear, concise messaging, plain language
- Credible sender, targeted audience
- Include disability communications



Redundant methods

- Internal alerts
- Responder notification
- External warnings

Evacuate? Lockdown? SIP?

Standard Response Protocol

HOLD
SECURE
LOCKDOWN
EVACUATE
SHELTER

OHNO – The Power of Hello

Alert employees can spot suspicious activity and report it.

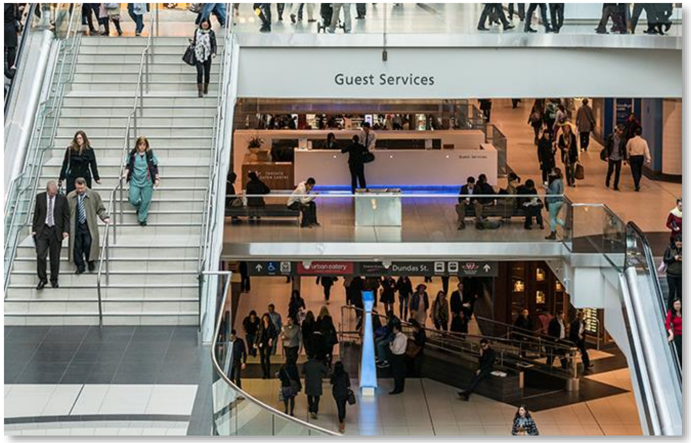
Observe - Initiate a **H**ello

Navigate the Risk - **O**btain Help

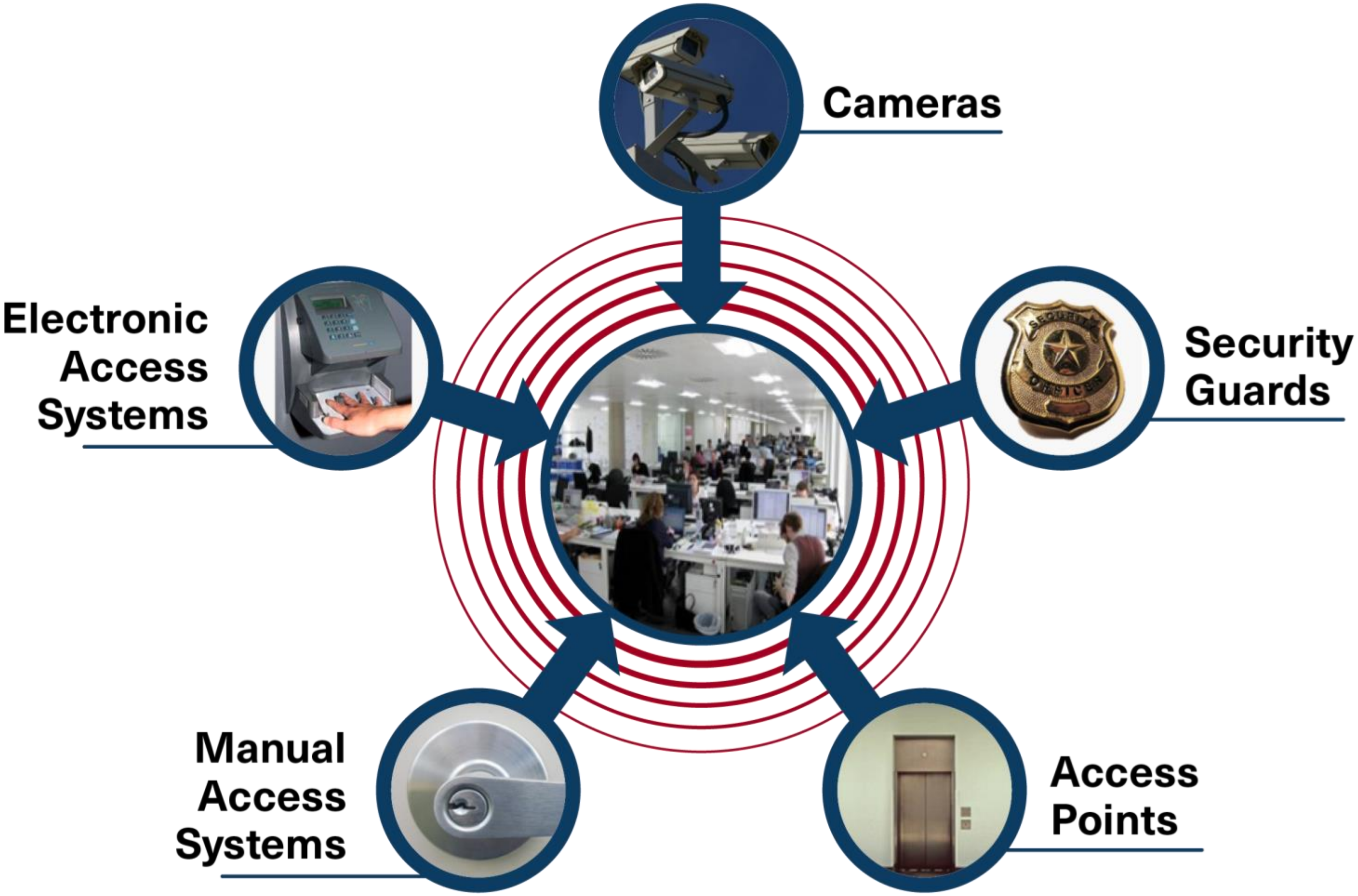
Protective Measures

Protection

- Evaluate security options appropriate for the occupancy
- Consider how building design affects planning
- Determine the policies and procedures necessary to secure the organization and its stakeholders against an active shooter



Security Measures



Cameras

Electronic Access Systems

Security Guards

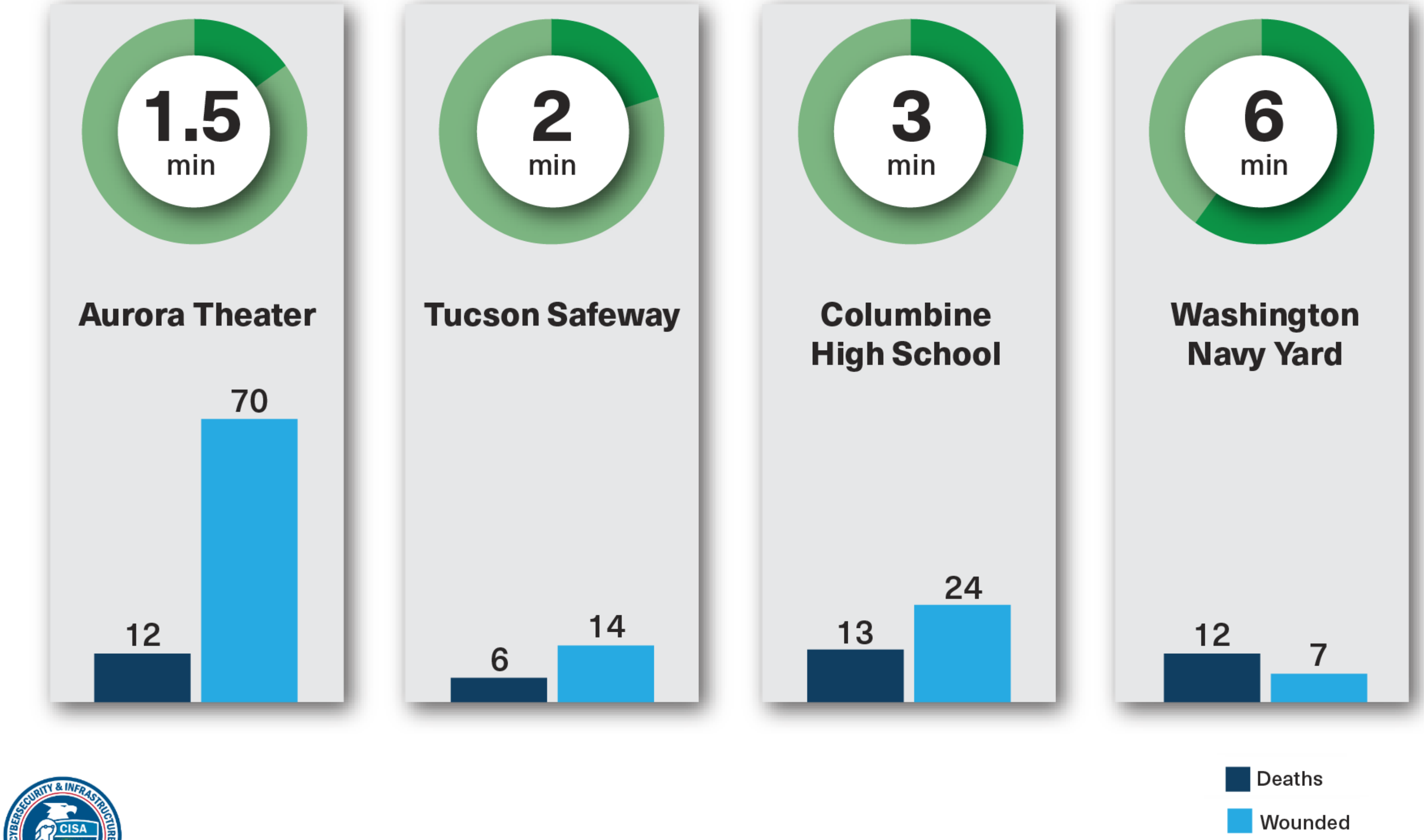
Manual Access Systems

Access Points

Protection & Security

- Incidents occur at both secured and open facilities.
- Physical security alone does not provide protection.
- Camera systems may not deter active shooters.
- Physical security needs to be paired with appropriate policies and procedures.
- Armed (vs. unarmed) guards are present.
- Building design plays a role in response to an incident.

Incident Response Times



Video: Options for Consideration

Stop the Bleed

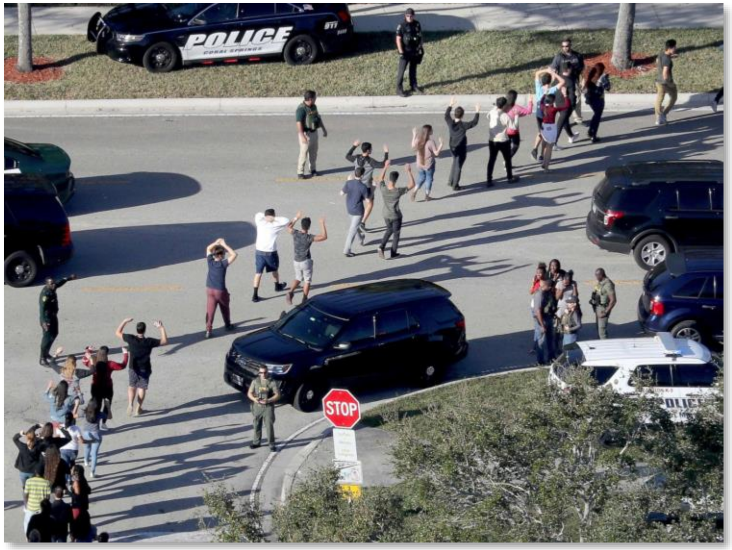
From Bystander to Immediate Responder

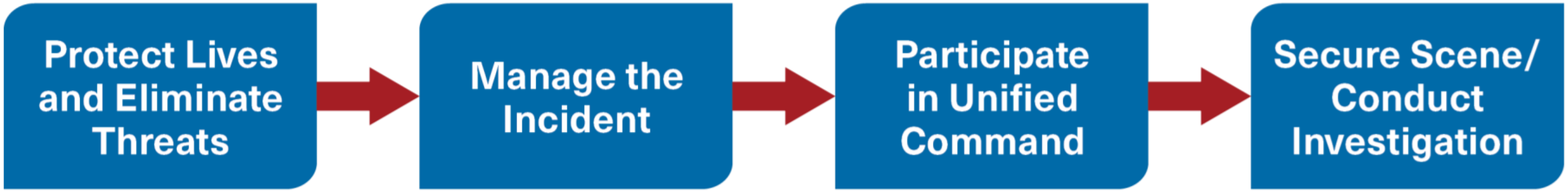
The person next to a bleeding victim may be the one most likely to save them

dhs.gov/stopthebleed

stopthebleed.org

Law Enforcement Priorities

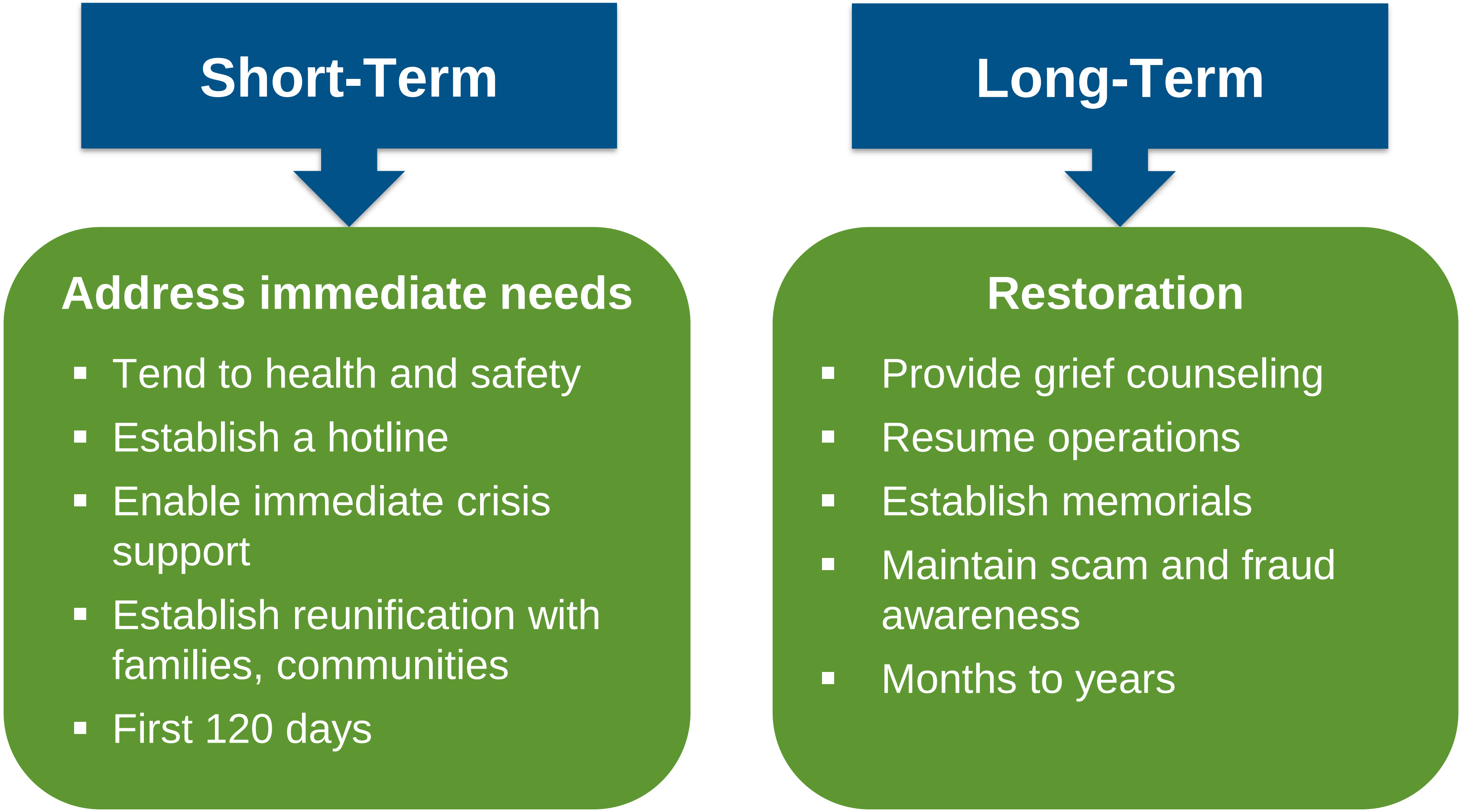



Protect Lives and Eliminate Threats → Manage the Incident → Participate in Unified Command → Secure Scene/ Conduct Investigation

First Officers on the Scene

- Sole focus is to go directly to the threat and eliminate it
- May be composed of multiple agencies
- Will be chaotic
- Obey all commands without delay

Recovery



Short-Term

Address immediate needs

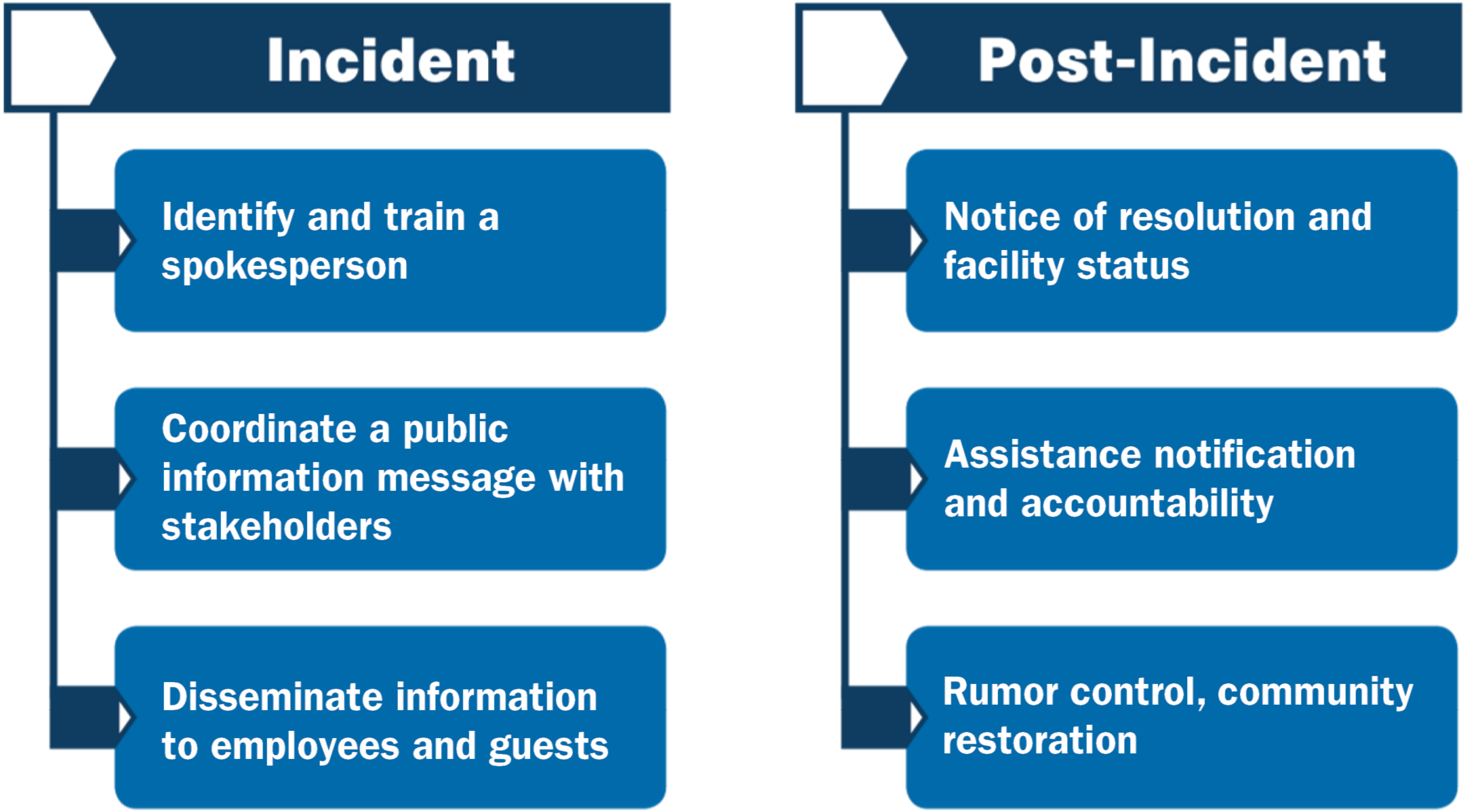
- Tend to health and safety
- Establish a hotline
- Enable immediate crisis support
- Establish reunification with families, communities
- First 120 days

Long-Term

Restoration

- Provide grief counseling
- Resume operations
- Establish memorials
- Maintain scam and fraud awareness
- Months to years

Coordinated Public Information



Incident

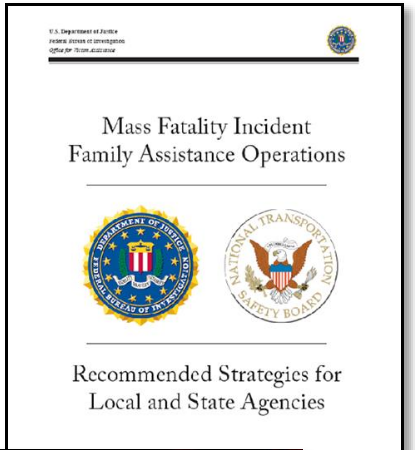
- Identify and train a spokesperson
- Coordinate a public information message with stakeholders
- Disseminate information to employees and guests

Post-Incident

- Notice of resolution and facility status
- Assistance notification and accountability
- Rumor control, community restoration

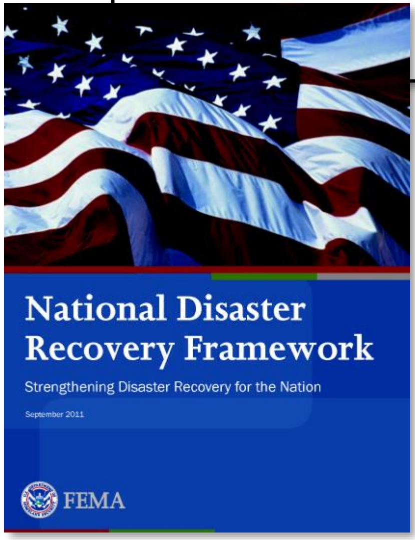
Recovery References

- Mass Fatality Incident Family Assistance Operations
- Active Shooter Healthcare Facility Emergency Operations
- Responding to Victims of Mass Crimes
- UCLA – Responding to a Crisis at School
- “I Love U Guys” Foundation – Reunification
- National Disaster Recovery Framework


U.S. Department of Justice
Federal Bureau of Investigation
Office for Victim Assistance

Mass Fatality Incident
Family Assistance Operations

Recommended Strategies for
Local and State Agencies


National Disaster
Recovery Framework

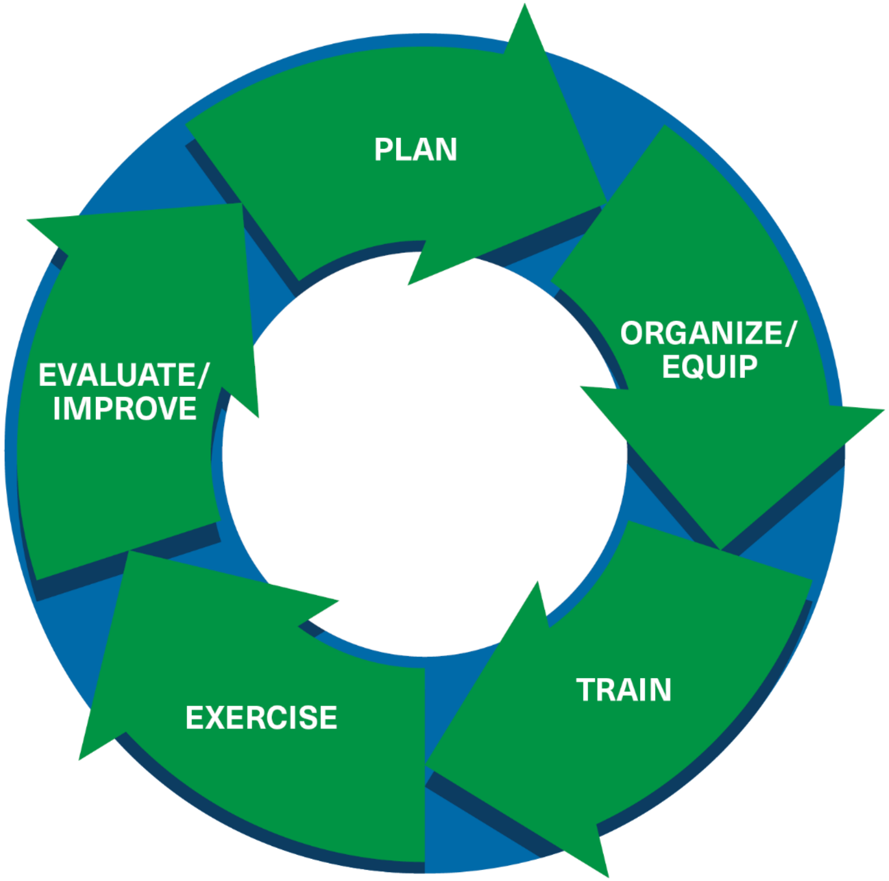
Strengthening Disaster Recovery for the Nation

September 2011

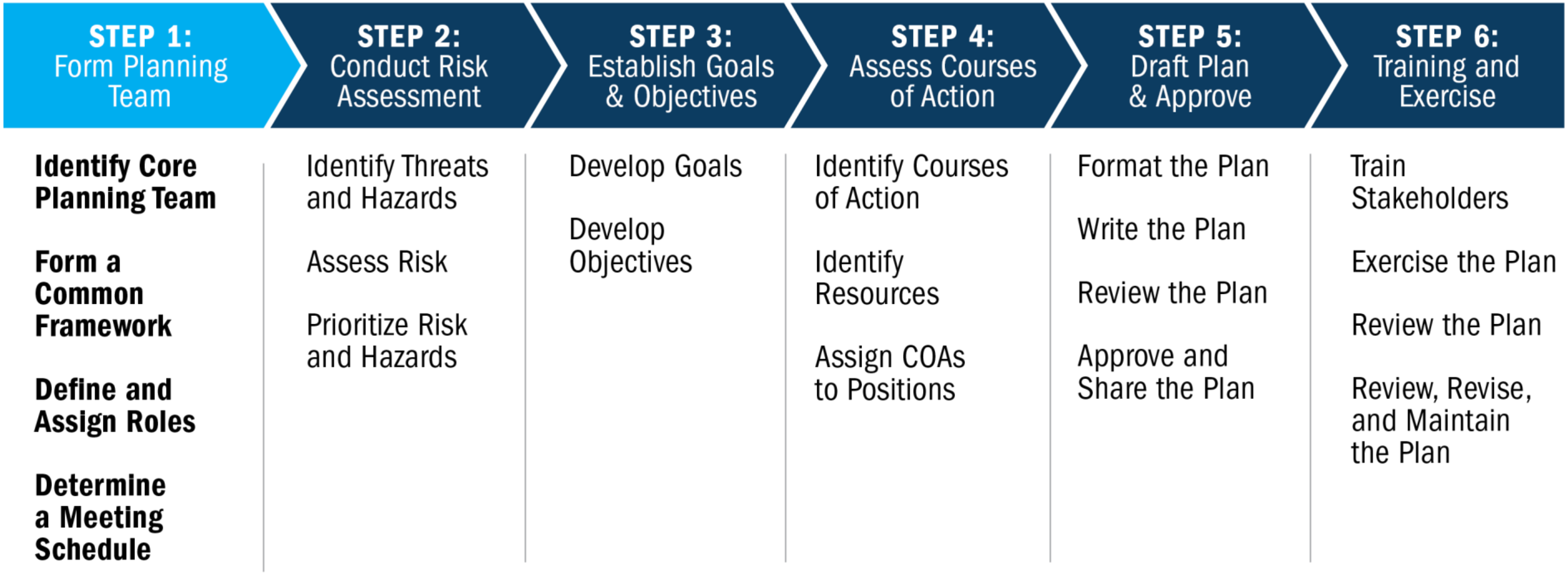
FEMA

Preparedness Cycle

The Preparedness Cycle is ongoing



Preparedness Plan Development



STEP 1:
Form Planning Team

- **Identify Core Planning Team**
- **Form a Common Framework**
- **Define and Assign Roles**
- **Determine a Meeting Schedule**

STEP 2:
Conduct Risk Assessment

- Identify Threats and Hazards
- Assess Risk
- Prioritize Risk and Hazards

STEP 3:
Establish Goals & Objectives

- Develop Goals
- Develop Objectives

STEP 4:
Assess Courses of Action

- Identify Courses of Action
- Identify Resources
- Assign COAs to Positions

STEP 5:
Draft Plan & Approve

- Format the Plan
- Write the Plan
- Review the Plan
- Approve and Share the Plan

STEP 6:
Training and Exercise

- Train Stakeholders
- Exercise the Plan
- Review the Plan
- Review, Revise, and Maintain the Plan

Training Materials

Independent study courses:

- IS 906: Workplace Security Awareness
- IS 907: Active Shooter: What You Can Do
- IS 914: Surveillance Awareness: What You Can Do
- IS 915: Protecting Critical Infrastructure Against Insider Threat

https://training.fema.gov/emi.aspx

Training Delivery

Use a variety of training avenues

New employee orientation

“All Hands” meetings

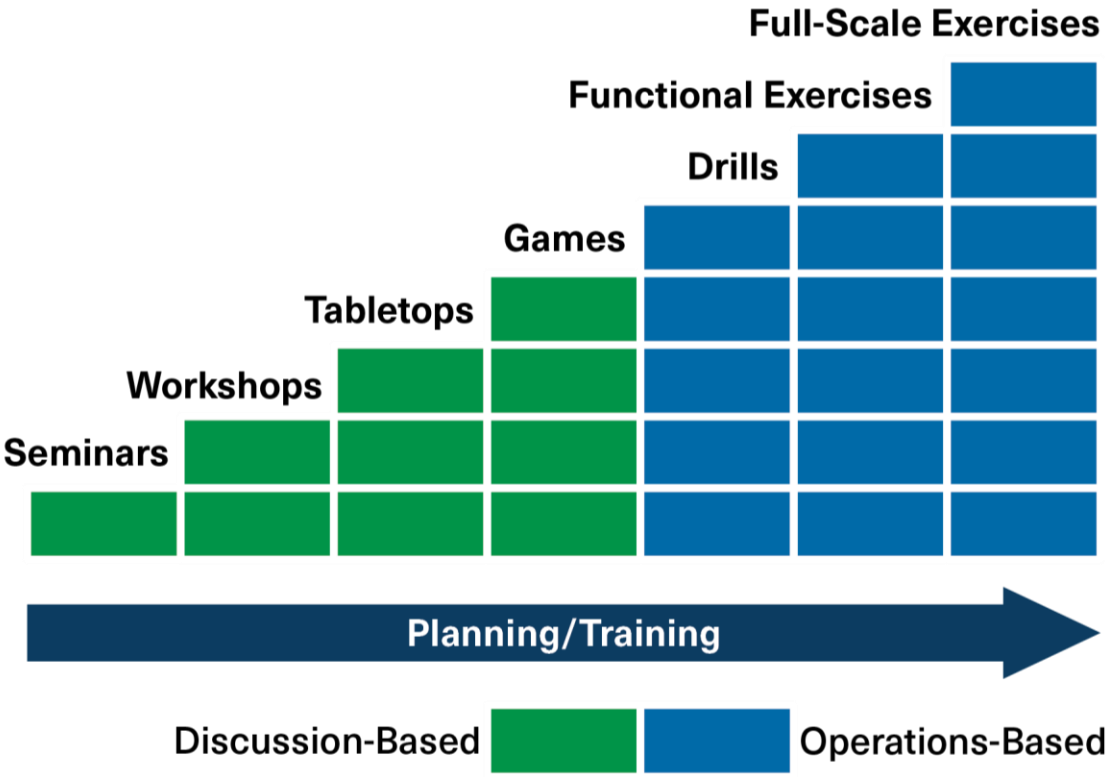
Conferences and workshops

Newsletters and internal broadcasts

Online courses

Include part-time employees and volunteers

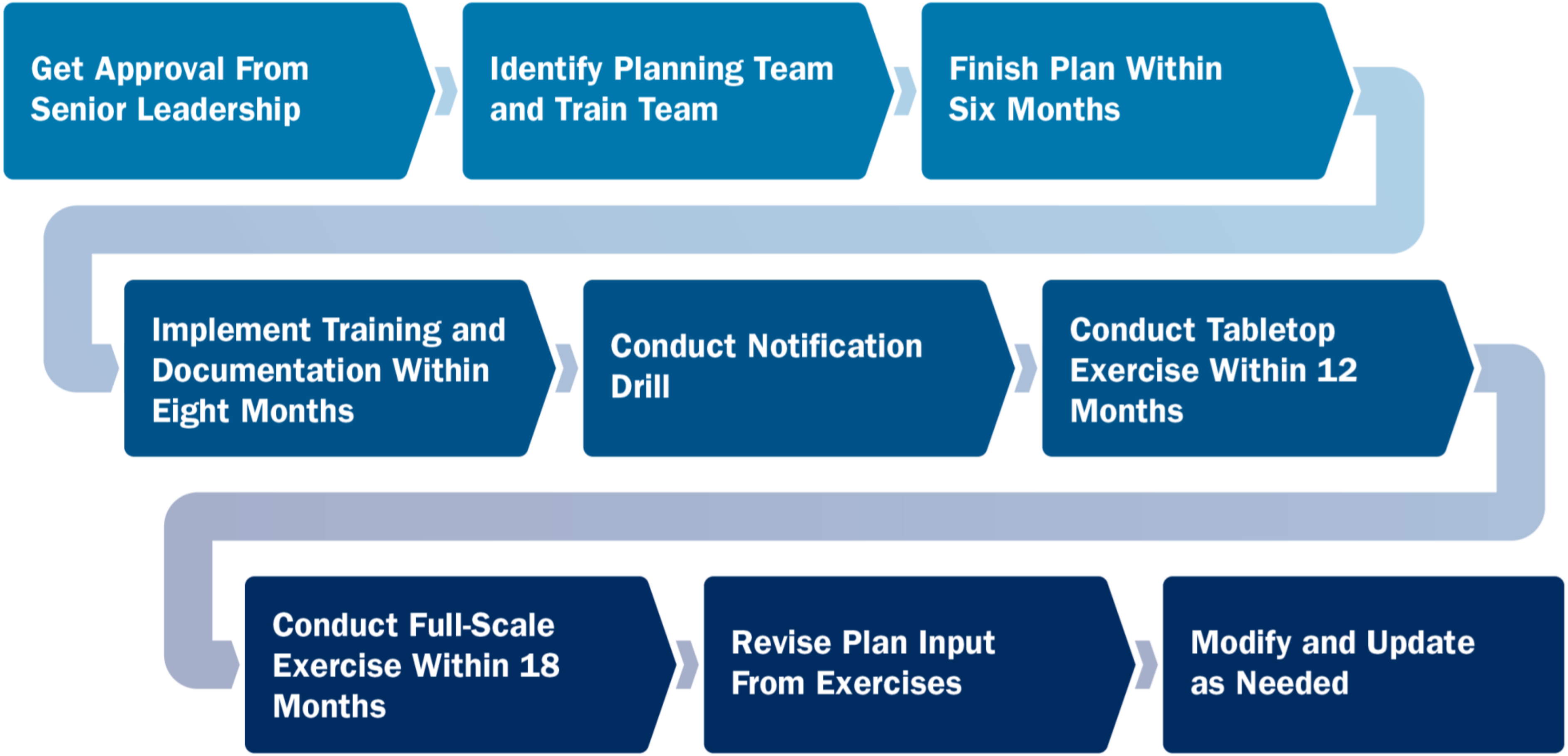
Progressive Approach



Regardless of exercise type, each builds on a set of common program priorities and tests capabilities

Homeland Security Exercise and Evaluation Program (HSEEP) FEMA March 2006

The Way Ahead



Get Approval From Senior Leadership

Identify Planning Team and Train Team

Finish Plan Within Six Months

Implement Training and Documentation Within Eight Months

Conduct Notification Drill

Conduct Tabletop Exercise Within 12 Months

Conduct Full-Scale Exercise Within 18 Months

Revise Plan Input From Exercises

Modify and Update as Needed

Active Shooter Preparedness Webinar

September 15, 2021 10:00 a.m.

Who Should Participate?

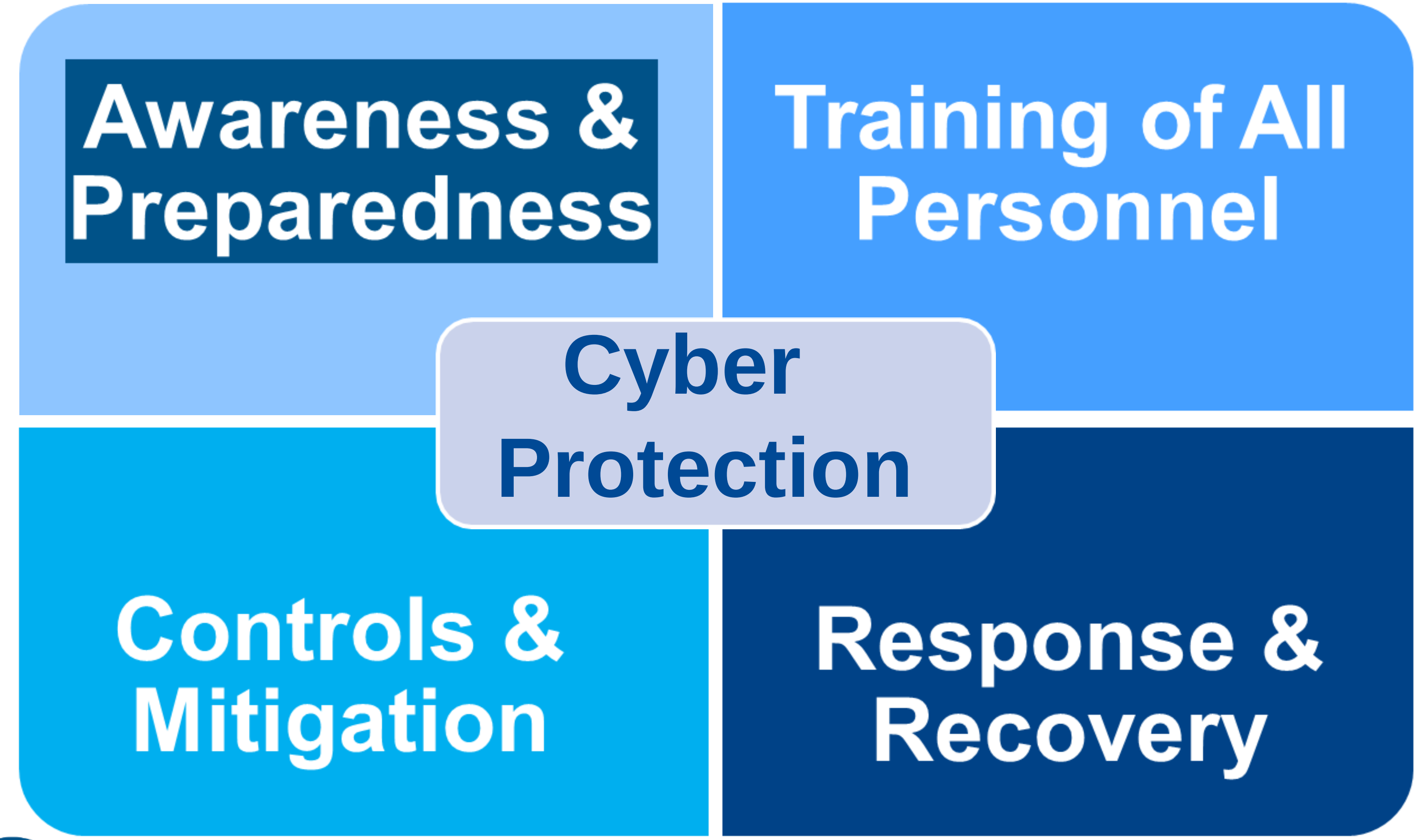
Anyone with a role in planning for, or managing an active shooter incident

- Private and public organizations
- Corporate and facility managers & security staff
- Human resource managers
- Community response officials
- Health organizations
- Faith-based leaders
- School administrators and security officers

Active Shooter Preparedness

- Virtual 2-hour webinars
- On-site training
- Site Assist Visit (SAV)
- Assessments
- Other resources

Cybersecurity



Awareness & Preparedness

Training of All Personnel

Cyber Protection

Controls & Mitigation

Response & Recovery

Cybersecurity Minimums

- Back up data
- Patch Tuesday
- Assessments
- Segmentation of network
- Test incident response plan
- Subscribe to information streams
- Train employees – social engineering - reporting

For more information:
cisa.gov

Questions?

Matt Beaudry– PSA, Utah
matthew.beaudry@cisa.dhs.gov
Phone: 801-837-8314